

Modelling knowledge security: knowledge security as a knowledge management problem

by
Christopher James Shear



*Dissertation presented for the degree of
Doctor of Philosophy in the Faculty of Arts and Social Sciences
at Stellenbosch University*

Supervisor: Prof. Bruce Watson
Co-supervisor: Dr Martin Van der Walt

December 2021

Declaration

By submitting this dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third-party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

December 2021

Copyright © 2021 Stellenbosch University
All rights reserved

Summary

For today's organisations, knowledge has become a highly valuable resource, one that is often critical for competitive success. As such, a variety of methods and approaches have surfaced in recent decades, coalescing into what has become known as knowledge management (KM). The purpose of KM is largely focused on using various mechanisms and technologies to promote the discovery, capture, sharing and application of knowledge to derive value. Yet, while many studies address how knowledge should be leveraged more openly, fewer have focused on how best to secure it. This poses a risk to organisations, due to the increasing complexity of the intelligence-gathering mechanisms employed by those seeking to gain this knowledge for their advantage.

In response, the idea of knowledge security has emerged as a mechanism to counter this risk. From an academic perspective, it has largely been grounded in information security theory. This has occurred because of the convergence that has taken place between information systems and KM, with security having taken a largely explicit focus. While beneficial in some ways, this approach is also somewhat problematic for a couple of reasons. Firstly, knowledge can extend beyond the explicit and is often found in intangible tacit forms, which may not be covered by taking a pure information security-driven approach. Thus, not having a comprehensive understanding of the measures needed to secure organisational knowledge at each dimension of KM activity, and vice versa, can make knowledge more vulnerable to compromise. Secondly, this creates a dichotomy between KM activity, predominantly centred on the amplification and distribution of knowledge and current security practices, which aim to limit and control access to processes. It is also a symptom indicative of the deeper question about knowledge in organisations, in terms of how it should best be retained, protected, and managed, in a balanced manner.

Thus, the study focuses on overcoming this discrepancy by imposing the meta-question of knowledge security upon KM theory. The objective of the research is to advance the body of knowledge, by contributing to it in the form of a better understanding of how knowledge security can be conceptualised as a KM problem and be presented as a model. It is hoped that in doing so, it will set the foundation for future research on this topic and that it will contribute to solidifying knowledge security as part of the broader set of KM processes. To achieve these research objectives, the research design is structured to focus on three components. The first is a theoretical analysis centred on an examination of the literature related to organisational

knowledge, KM, and knowledge security. The second is an empirical analysis focused on identifying the relationship between security and knowledge in practice. The third is combining the insights gained from the first two components and using these inputs to design a conceptual model outlining the relationship between knowledge security and KM. This process culminated in the development of a conceptual model of knowledge security that highlights its relationship with KM.

Opsomming

Vir hedendaagse organisasies het kennis 'n baie waardevolle hulpbron geword wat dikwels van kritieke belang is vir mededingende sukses. As sodanig, het 'n verskeidenheid metodes en benaderings die afgelope dekades opgeduik, wat saamgegroeï het in wat bekend geword het as kennisbestuur (KB). Die doel van KB is gefokus op die gebruik van verskillende meganismes en tegnologieë om die ontdekking, vaslegging, deel en toepassing van kennis ten einde waarde te verkry, te bevorder. Alhoewel daar baie studies is oor hoe kennis openliker gebruik moet word, het minder gefokus op die beste manier om dit te beveilig. Dit hou 'n risiko in vir organisasies as gevolg van die toenemende kompleksiteit van die intelligensie-insamelingsmeganismes wat gebruik word deur diegene wat hierdie kennis vir hul eie voordeel wil verkry.

In reaksie hierop het die idee van kennisbeveiliging na vore gekom as 'n meganisme om hierdie risiko teë te werk. Vanuit 'n akademiese perspektief is dit grotendeels gegrond in die teorie oor inligtingsekuriteit. Dit het plaasgevind as gevolg van die konvergensie wat tussen inligtingstelsels en KB plaasgevind het, met veiligheid wat grotendeels eksplisiet gefokus het. Alhoewel dit op sommige maniere voordelig is, is dit om 'n aantal redes ook ietwat problematies. Eerstens, kan kennis verder strek as die eksplisiete en word dikwels in ontasbare, stilswyende vorms aangetref, wat miskien nie gedek word deur 'n suiwer inligtingsekuriteits gedrewe benadering te volg nie. Tweedens, skep dit 'n tweespalt tussen KB-aktiwiteit, wat hoofsaaklik gerig is op die versterking en verspreiding van kennis, en huidige veiligheidspraktyke, wat daarop gemik is om toegang tot prosesse te beperk en te beheer. Dit is ook 'n simptome wat aandui op die diepere vraag oor kennis in organisasies, in terme van hoe dit die beste op 'n gebalanseerde manier behou, beskerm en bestuur kan word.

Die studie fokus dus op hoe om hierdie teenstrydigheid te oorkom deur die meta-vraag oor kennisbeveiliging aan die KB-teorie op te lê. Die doel van die navorsing is om die liggaam van kennis te bevorder deur daartoe by te dra in die vorm van 'n beter begrip van hoe kennisbeveiliging as 'n KB-probleem gekonseptualiseer kan word en as 'n model aangebied kan word. Daar word gehoop dat dit die grondslag sal lê vir toekomstige navorsing oor hierdie onderwerp en dat dit sal bydra tot die verstewiging van kennisbeveiliging as deel van die breër reeks KB-prosesse. Om hierdie navorsingsdoelstellings te bereik, is die navorsingsontwerp gestruktureer om op drie komponente te fokus. Die eerste is 'n teoretiese analise wat fokus op 'n ondersoek van die literatuur wat verband hou met organisasiekennis, KB en

kennisbeveiliging. Die tweede is 'n empiriese analise wat fokus op die identifisering van die verband tussen sekuriteit en kennis in die praktyk. Die derde is die kombinasie van die insigte wat verkry is uit die eerste twee komponente en die gebruik van hierdie insette om 'n konseptuele model te ontwerp wat die verband tussen kennisbeveiliging en KB uiteensit. Hierdie proses het uitgeloop op die ontwikkeling van 'n konseptuele model van kennisbeveiliging wat die verhouding met KB beklemtoon.

Acknowledgements

Firstly, I would like to thank my supervisors Prof. Bruce Watson and Dr Martin Van der Walt for their invaluable help, advice, and support in completing my PhD research. Secondly, I would like to thank my late supervisor, Prof. Hans Müller, for helping me to conceptualise this project and Prof. Johann Kinghorn for stepping in to assist in the very difficult time after his passing. Thirdly, I would like to thank Dr Endicott-Popovsky and Dr Slava Popovsky for their insight and the incredible opportunities they afforded me to extend my knowledge in practice and academia. Their kindness made a world of difference to my research, and I am very grateful. Fourthly, I would like to express my gratitude to all the participants who took time out of their schedules to participate in my research interviews and who provided some very valuable insights. Fifthly, I would like to thank all my friends and family who supported me in so many ways. Without their incredible help, understanding and encouragement over the past years, I would not have been able to complete this dissertation. Finally, I would like to thank those organisations who helped to support this research financially. The research was partially supported by a National Research Foundation (NRF) grant, a grant from the Centre for Artificial Intelligence Research (CAIR) at Stellenbosch University, a scholarship for overseas study from Stellenbosch University and an Oppenheimer scholarship.

Dedications

I dedicate this dissertation to my late mother Mrs Maureen Shear. Although she did not get to see me finish this degree, the courage she showed in her life motivated me to keep going through the most difficult of times. I am forever grateful for all that she did for me and the inspiration she continues to be.

Table of Contents

List of Figures	xi
List of Tables.....	xii
List of Abbreviations	xiii
Chapter 1 Introduction	1
1.1 Background	1
1.2 Research Problem	6
1.2.1 Research Statement and Questions.....	7
1.3 Research Design.....	7
1.3.1 Theoretical Analysis.....	8
1.3.2 Empirical Analysis	9
1.4 The Importance of the Study	10
1.5 Chapter Layout.....	10
Part 1 – Theoretical Analysis.....	13
Chapter 2 Defining Organisational Knowledge	14
2.1 Introduction	14
2.2 Core Definitions of Knowledge	14
2.2.1 Normalising Definitions of Knowledge	16
2.2.2 A Tacit and Explicit View of Knowledge Definitions	19
2.2.3 Normalising Knowledge Definitions Through a Tacit and Explicit Framework.....	21
2.2.4 Key Issues of Knowledge from an Organisational Perspective.....	33
2.3 Adopting a Definition of Organisational Knowledge	38
2.3.1 Overview of Tsoukas’ Definition of Organisational Knowledge	44
2.3.2 The Risks and Benefits of Using Tsoukas’ Definition of Organisational Knowledge	49
2.4 Conclusion	51
Chapter 3 Defining Knowledge Management	52
3.1 Introduction	52
3.2 The Rise in Importance of Knowledge Management.....	52
3.3 Key Theoretical Positions in Knowledge Management	56
3.4 The Problem with Defining Knowledge Management.....	64
3.5 Consolidating Definitions of Knowledge Management	66
3.5.1 Limitations of the Approach.....	73
3.6 Conclusion	74
Chapter 4 Literature Review of Knowledge Security Approaches	75
4.1 Introduction	75

4.2	The Need to Integrate Knowledge Security with Knowledge Management	75
4.3	The Need for Knowledge Security	81
4.4	Identifying Knowledge Security Paradigms.....	86
4.4.1	Step 1 – Identifying Relevant Literature	88
4.4.2	Step 2 – Categorising the Literature	90
4.4.3	Step 3 – Discussing the Literature	93
4.5	Conclusion	124
Part 2 – Empirical Analysis		125
Chapter 5 Review of Knowledge Security in Leading Academic Programs.....		126
5.1	Introduction	126
5.2	Identifying Relevant Universities.....	126
5.2.1	The Identification Process	127
5.2.2	The Filtering and Aggregation Process	130
5.3	Analysis of Selected Universities.....	132
5.3.1	USA Universities Results and Findings	134
5.3.2	EUR Universities Results and Findings	138
5.4	Discussion of Findings	141
5.4.1	General Observations of the Findings	141
5.4.2	Validity of Original Assumptions Made.....	142
5.4.3	Limitations of the Research and Analysis	143
5.5	Conclusion	144
Chapter 6 Review of Knowledge Security in Practice		146
6.1	Introduction	146
6.2	Research Design.....	146
6.2.1	Research Paradigm	147
6.2.2	Case-Based Research	149
6.2.3	Unit of Analysis.....	150
6.2.4	Selection of Cases	151
6.3	Research Method.....	160
6.3.1	Data Collection.....	161
6.3.2	Ethics.....	163
6.3.4	Analysis and Interpretation.....	166
6.3.5	Case Study Narratives.....	168
6.4	Cross-Case Analysis and Discussion of Findings	181
6.4.1	General Observations	181
6.4.2	Alignment with Academic Teaching	181

6.4.3	Additional Knowledge Security Considerations	184
6.4.4	Limitations of the Study	187
6.5	Conclusion	187
Part 3 – Conceptual Model		189
Chapter 7 Modelling Knowledge Security as a Knowledge Management Problem		190
7.1	Introduction	190
7.2	Selecting a Conceptual Modelling Approach.....	190
7.2.1	Brief Overview of Conceptual Modelling	191
7.2.2	Conceptual Modelling as Applied to Knowledge Management	193
7.2.3	Choosing an Approach to Conceptual Modelling	193
7.2.4	Overview of Conceptual Models in Knowledge Security	198
7.3	Developing a Conceptual Model of Knowledge Security	201
7.3.1	Establishing the Objectives of the Model.....	201
7.3.2	Reviewing Sources of Information.....	201
7.3.3	Extracting Relevant Model Inputs.....	202
7.3.4	Integrating Relevant Inputs into a Model	212
7.3.5	Discussion and Implications.....	222
7.4	Limitations of the Model.....	233
7.5	Recommendations for Future Research	234
7.6	Conclusion	235
Appendices – Appendix A		272
A	Semi-Structured Interview Question Guide	272
A1	Overview of Knowledge Management.....	272
A2	Knowledge Discovery	272
A3	Knowledge Capture.....	272
A4	Knowledge Sharing	273
A5	Knowledge Application.....	273
A6	Examining Links Between Academia and Practice	274

List of Figures

Figure 1-1: Overview of Becerra-Fernandez and Sabherwal's Model of KM Solutions.....	5
Figure 1-2: Structure of the Study	11
Figure 4-3: Manhart and Thalmann's Literature Review Process	87
Figure 4-4: Adapted Literature Review, Categorisation and Discussion.....	88
Figure 7-5: Conceptual Model of Knowledge Security Framed as a KM Problem.....	217

List of Tables

Table 2-1: Taxonomies of Knowledge	17
Table 2-2: Knowledge Definitions & Their Relationship to Key Organisational Knowledge Issues	38
Table 3-3: List of KM Definitions Chosen from the Academic Literature	69
Table 3-4: A Comparison of the Most Common Words Relating to KM Definitions	72
Table 4-5: Categorisation-Based Concept Matrix of Paradigms, Perspectives and Authors	94
Table 4-6: Ranking of Important Issues in Secure KM Research by Park <i>et al.</i>	121
Table 5-7: List of Identified Institutions per Ranking Body	129
Table 5-8: Filtering Matrix Used to Select the Final Universities for Analysis	131
Table 5-9: Aggregated Lists of USA and EUR Universities	132
Table 6-10: List of Identified MAKE 2015-2017	153
Table 6-11: List of Identified MIKE Winners 2018-2019	154
Table 6-12: Consolidated List of Identified MIKE and MAKE Organisations	155
Table 6-13: Alignment with Academic Teaching	182
Table 7-14: Examples of Conceptual Modelling Approaches in KM	194
Table 7-15: Summary of KM Conceptual Modelling Steps and their Popularity	196
Table 7-16: My Selected Conceptual Modelling Approach in Relation to KM Modelling Steps	197
Table 7-17: Summary of Model Inputs Derived from the Analysis of the Chapters	203
Table 7-18: The Main Aspects Followed by Experts When Creating Conceptual Models	214
Table 7-19: Illustrative Examples of Model Sub-Concepts	218

List of Abbreviations

AI	Artificial Intelligence
AIIM	Association for Intelligence Information Management
CIA	Confidentiality Integrity and Availability
COPs	Communities of Practice
COVID-19	Coronavirus Disease 2019
CSFs	Critical Success Factors
DIS	Defence and Intelligence Sector
EUR	European Region
HR	Human Resources
IAEA	International Atomic Energy Agency
ICT	Information and Communication Technology
IMF	International Monetary Fund
IP	Intellectual Property
IT	Information Technology
ITSM	Information Technology Security Management
KEI	Knowledge Economy Index
KM	Knowledge Management
KMS	Knowledge Management System
KSRM	Knowledge Security Risk Management
MIKE	Most Innovative Knowledge Enterprise
NDA	Non-disclosure Agreement
NIST 800-53	National Institute of Standards and Technology Special Publication 800-53
NSTISSC	National Security Telecommunications and Information Systems Security Committee Model
OCTAVE-S	Operationally Critical Threat, Asset and Vulnerability Evaluation – Small
OSINT	Open-Source Intelligence Gathering
QS	Quacquarelli Symonds
RDF	Resource Description Framework
RFID	Radio Frequency Identification
ROI	Return on Investment
SECI	Socialisation Externalisation Combination and Internalisation
SHAMAN	Sustaining Heritage Access Through Multivalent Archiving
SKM	Secure Knowledge Management
SOP	Standard Operating Procedure

THE	Times Higher Education
USA	United States of America
XML	Extensible Mark-Up Language

Chapter 1

Introduction

1.1 Background

Today we live in a world where knowledge has risen to a place of prominence in our society and economy as never before¹. The effects of this rise can be observed in the rapid changes that have swept society in recent decades, in the form of technological, economic, occupational, spatial, and cultural shifts^{2 3}. These shifts have resulted in the manifestation of what has become known as the knowledge society and economy⁴. Therefore, it is hardly surprising that for organisations operating within the knowledge economy⁵, knowledge has become an extremely valuable and strategically significant resource⁶. Viewed from this perspective, organisations have in essence become knowledge-based systems⁷, which rely on it for their continued innovation, strategic decision making and competitive success⁸.

To deal with the organisational challenges that these shifts have brought, a variety of methods and approaches have surfaced in recent decades, focused on how best to manage knowledge⁹. Collectively, within the body of organisational knowledge literature¹⁰, these methods and approaches have coalesced into what is known as knowledge management (KM). Some of the benefits of adopting KM by organisations have been improved productivity and effectiveness; improved efficiency and cost savings; increased responsiveness; better communication;

¹ Webster, 2006. *Theories of the Information Society* p 2.

² Webster, 2006. *Theories of the Information Society* p 8-21.

³ Chen & Lee, 2004. *The New Knowledge Economy of Taiwan* p 2-17.

⁴ Dubina *et al.*, 2012. *Creativity Economy and a Crisis of the Economy? Coevolution of Knowledge, Innovation, and Creativity, and of the Knowledge Economy and Knowledge Society* p 1.

⁵ Powell & Snellman, 2004. *The Knowledge Economy* p 201.

⁶ Zack, 1999. *Developing a Knowledge Strategy* p 134.

⁷ Tsoukas, 2005. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 21.

⁸ Neef *et al.*, 1998. *The Economic Impact of Knowledge* p 175.

⁹ Wiig, 1997. *Knowledge management: Where Did it Come from and Where Will it Go?* p 6-7.

¹⁰ Wiig, 1997. *Knowledge management: Where Did it Come from and Where Will it Go?* p 6-7.

innovation; better employee retention; and increased market share¹¹. Thus, the leveraging of knowledge, for competitive advantage, continues to be promoted as a means of rising to the challenges posed by the knowledge economy.

Yet, while many studies address how knowledge should be leveraged by organisations, little has been formally outlined about how best to secure it. This is particularly evident when examining how security can be aligned with an organisation's objectives from a KM paradigm¹². From within the literature, most of those studies that do tackle the issue of securing organisational knowledge are predominantly grounded in traditional information systems security theory. For example, apart from a few studies focused on defence and intelligence sector (DIS) theory¹³, most are focused on information technology (IT) systems, governance, and risk paradigms.

Aiming to secure organisational knowledge, through what are largely technically focused mechanisms, can be problematic. This is because, unlike information that is predominantly managed through IT systems and is tangible, organisational knowledge can extend beyond tangible forms, often existing as intangible tacit knowledge¹⁴. Additionally, the problem is compounded further as less IT systems inclined KM authors, like Snowden or Takeuchi¹⁵, do not even speculate about knowledge security in their arguments. Instead, they focus more on learning and openness rather than on how knowledge could be secured as part of KM. Authors such as Desouza and Vanapalli, who do have a knowledge security focus, try to overcome this shortfall by outlining the common practices of knowledge security used by DIS organisations, conducting KM¹⁶. However, how these practices should be transitioned to the private sector¹⁷ is not defined. Thus, having coined the notion of knowledge security, it has not translated into developing an integrated conceptualisation of what knowledge security should mean for organisations.

¹¹ Nevo & Chan, 2007. *A Delphi Study of Knowledge Management Systems: Scope and Requirements* p 590.

¹² Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 85.

¹³ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 96-97.

¹⁴ Clarke & Clegg, 2000. *Changing Paradigms: The Transformation of Management Knowledge for the 21st Century* p 340.

¹⁵ Takeuchi, 2001. *Towards a Universal Management Concept of Knowledge* p 315-329.

¹⁶ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 86.

¹⁷ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 96-97.

Further, the importance and difficulty of securing organisational knowledge from a KM perspective is not to be underestimated. As Desouza and Vanapalli state, “organizations must pay due diligence to the concept of security in terms of protecting and managing their most valuable resource – knowledge”¹⁸. Competitors are making use of ever more sophisticated strategies¹⁹, employing government intelligence style practices to obtain the knowledge they seek²⁰. The resultant implications of these trends can be quite substantial^{21 22}. If the matter is approached from the more fundamental perspective of KM, this issue becomes not only important but also infinitely more complex²³.

Another concern relating to this issue is that protecting tacit knowledge in organisations is always going to be a problem. This is because the vulnerability of tacit knowledge is dependent on the often-unpredictable actions of those individuals who possess it. To overcome this challenge, current security approaches, such as those outlined in the DIS, emphasise controlling employees’ actions. For example, using surveillance and monitoring mechanisms as a means of deterrence²⁴. However, taking such an approach, when applied to employees in this way, is potentially flawed. McGregor argues, in his *Theory X and Theory Y*²⁵, if employees are treated in a controlling manner, and the culture is not supportive of this, they may inherently seek to find loopholes to such control mechanisms. This poses a risk, as employees may intentionally attempt to find loopholes to being monitored, thereby risking the confidentiality of their knowledge. Thus, a vulnerability will be created by the very process of monitoring that the organisation has put in place to protect its knowledge.

Therefore, from a knowledge security perspective, when thinking about KM, it will be important to assess the type of organisational culture at play. It will also be important to determine how this culture aligns with the broader strategic focus of the organisation and if employees are aware of the possible ramifications of their actions. Such discussions, in terms

¹⁸ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 97.

¹⁹ Whitehead, 2001. *The Counterintelligence Page: Part 1* p 32.

²⁰ Whitehead, 2001. *The Counterintelligence Page: Part 1* p 32.

²¹ Whitehead, 2001. *The Counterintelligence Page: Part 1* p 32.

²² Kitfield, 2007. *Espionage the Sequel* [Online].

²³ Gold et al., 2010. *Knowledge Management: An Organizational Capabilities Perspective* p 207.

²⁴ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 99.

²⁵ McGregor, 1971. *Theory X and Theory Y, in Organisation Theory: Selected Readings* p 231.

of organisational culture and strategic focus, are something that will have to be included in knowledge security practices if KM risks are to be minimised effectively.

In the light of these trends, it appears that organisations are starting to take such issues seriously. This is indicated by the relatively recent emergence of the practices of competitive intelligence²⁶, business intelligence²⁷, and the notion of business counterintelligence²⁸. However, these practices are response mechanisms and do not allow one to seriously reconceptualise theory. Rather, they can be viewed as symptomatic of the deeper question about knowledge in organisations. This is in terms of how knowledge should best be retained, protected, and managed, in a balanced manner, for competitive success. As such, they are implemented without a comprehensive understanding of how they relate to the broader issues of KM in organisations.

Desouza and Vanapalli²⁹ contend that if knowledge security is to be developed successfully, it needs to be integrated with KM activity. As KM is made up of many different perspectives, maybe even being a diffused entity³⁰, this cannot be done unless it is underpinned with an integrated foundation of KM. The foundation needs to take a view on the literature and the perspectives of KM practically. Becerra-Fernandez and Sabherwal³¹ have developed such a view that consolidates the various KM perspectives into an integrated set of KM solutions³². This integrated descriptive model acts like a spreadsheet of intra-organisational knowledge activity. It also gives one a practical tool to identify those dimensions where knowledge security issues will feature prominently within the realm of KM. An overview of Becerra-Fernandez and Sabherwal's model is provided in Figure 1-1³³.

²⁶ Murphy, 2005. *Competitive Intelligence: Gathering, Analysing and Putting it to Work* p 6.

²⁷ Kerr, 2007. *Practical ways for Competitive Intelligence Professionals to Measure their Success* [Online].

²⁸ Shear, 2009. *Business Counterintelligence: Sustainable Practice or Passing Fad?* p 56.

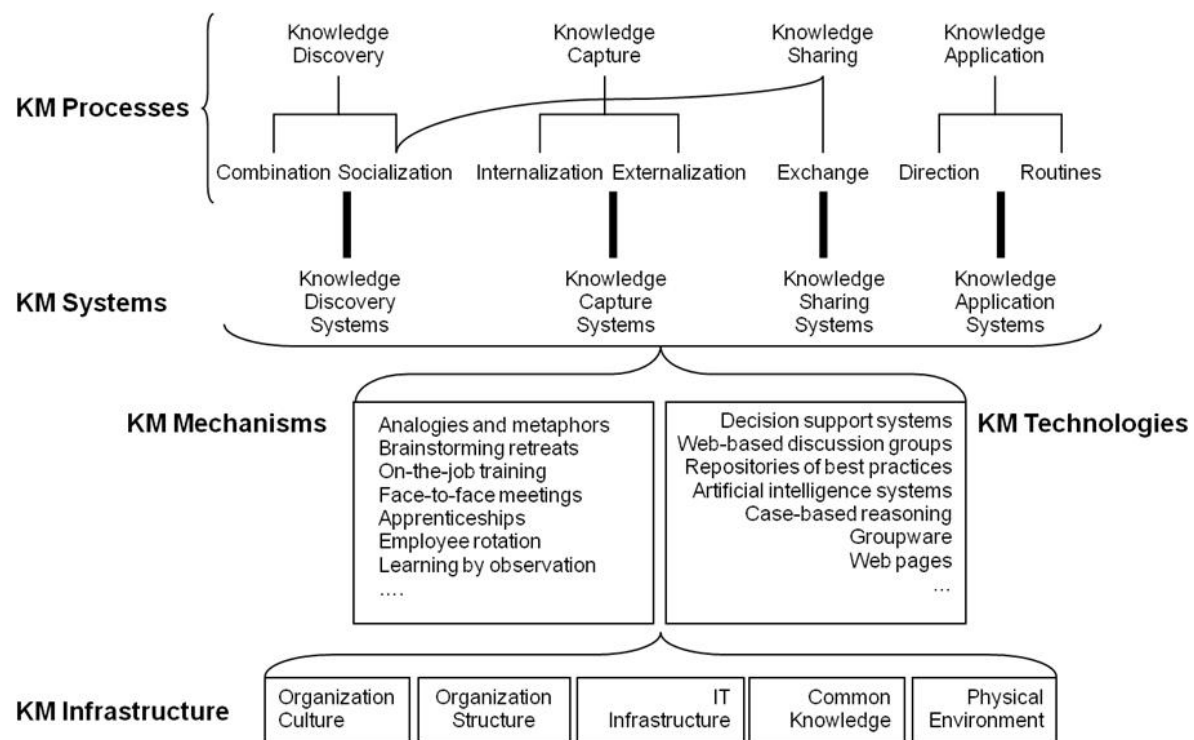
²⁹ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 96-97.

³⁰ Prusak & Snowden, 2008. *Is Knowledge Management Dead?* [Online].

³¹ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 66-68.

³² Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 66-68.

³³ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 68.

Figure 1-1: Overview of Becerra-Fernandez and Sabherwal's Model of KM Solutions

As the model is generally accepted to be a comprehensive representation of KM activity in organisations³⁴, I will be able to use it to determine how knowledge security will apply to the selected dimensions. From a security perspective, the identification of any risks and the application of security controls will need to be assessed within the broader areas of the model. These areas will include the KM Processes, KM Systems, KM Mechanisms, KM Technologies, and KM Infrastructure³⁵ as represented in the model. Thus, this appears to be the best way to align knowledge security practices comprehensively with KM activity.

Although the model is a good representation of KM activity in organisations, in the context of the study, it is not entirely without flaw. A problem with this model is that it is agnostic in terms of how it defines knowledge. Therefore, it can stand outside the raging debate about what the knowledge is, that is to be managed. This is not a sustainable position in the long run and not in the development of the notion of knowledge security. Even if I am to argue that knowledge security will be at stake in a variety of different practices and dimensions of KM, this does not solve the problem. For example, the implication of tacit knowledge as a notion

³⁴ Gibson cited in Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p xi-xii.

³⁵ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 68.

means that knowledge security will mean something quite different in this regard, then when new product design knowledge is at stake.

For this reason, I envisage that the development of the notion of knowledge security will require the further development of a position on the nature of the knowledge that is to be managed. Even if the final position attempts to be as encompassing as that of Becerra-Fernandez and Sabherwal, the detail of such a position will require a deeper investigation of the different constitutive types of organisational knowledge and KM theory.

1.2 Research Problem

Two problem areas come to mind when examining the issue of knowledge security and management. Firstly, as has been established, the importance of securing organisational knowledge from competitive threats is not to be underestimated. However, a discrepancy exists in that there is a lack of theory linking the concepts of knowledge security and KM activity in organisations. This creates a dichotomy between KM activity, predominantly centred on the amplification and distribution of knowledge and current security practices which aim to limit and control access to processes.

Secondly, not having a comprehensive understanding of the measures needed to secure organisational knowledge at each dimension of KM activity, and vice versa, makes knowledge more vulnerable and places it at risk. This risk is further compounded by the increasing complexity of intelligence gathering mechanisms employed by those seeking to gain knowledge for competitive advantage in today's knowledge economy.

Thus, the study will focus on overcoming these discrepancies, by imposing the meta-question of knowledge security upon organisational KM theory. As KM theory is broad and varied, I will frame this analysis using Becerra-Fernandez and Sabherwal's model of a detailed view of KM solutions³⁶, to determine the scope of the project. The use of this model will allow for a discretionary approach to knowledge in organisational settings, as without the use of a model everything is grey. The model will give me a practical tool to identify those knowledge dimensions where knowledge security will feature prominently. The inputs for the model will also be derived from an empirical element to the study, where I will determine to what extent organisations focus on knowledge security in the selected KM dimensions. Armed with this data and in conversation with similar work done elsewhere, I will have the necessary inputs to

³⁶ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 68.

construe a meta-theory of knowledge security, and its relationship with KM, in the form of a balanced conceptual model.

1.2.1 Research Statement and Questions

Based on the research problem, as outlined above, the primary research question and its corresponding sub-questions have been formulated as follows:

Primary Question:

1.1 How can knowledge security be conceptualised as a KM problem and presented as a model?

Sub-Questions:

2.1 How can knowledge be thought about and defined from the organisational perspective?

3.1 What are the key theoretical issues and positions in the literature as they relate to KM and how can it be defined?

3.2 Why is there a need to integrate knowledge security with KM?

4.1 What security approaches are expressed in the literature that focus on KM and how can they be categorised?

4.2 Why is there a need for knowledge security?

5.1 Are knowledge and security treated as separate entities in teaching and academic programs at leading universities?

6.1 Does what is done in practice reflect the elements found in academic teaching?

6.2 What is the relationship between KM and security in practice?

7.1 How can knowledge security be modelled conceptually as a KM problem and be presented as a model?

1.3 Research Design

Given that the study deals predominantly with theory, it aims to function at a higher level of abstraction. Thus, it is not about the analysis of empirical research data in a strict sense. Mouton states that research can be framed within three interlinking worlds consisting of “pragmatic

interest (everyday life), epistemic interest (science) and critical interest (meta-science)”³⁷. Due to the objective of this study being one of conceptual model development, its focus is on elements of epistemic and critical interest, with meta-science dominating. To achieve my research objectives, my research design focuses on three components. The first is a theoretical analysis centred around an examination of the literature related to organisational knowledge, KM, and knowledge security. The second is an empirical analysis focused on identifying the relationship between security and knowledge in practice. The third is combining the insights obtained from the first two components and using these inputs to design a conceptual model outlining the relationship between knowledge security and KM.

1.3.1 Theoretical Analysis

The study began by outlining and examining the literature in greater detail. The purpose of doing so was to better understand organisational knowledge, KM, and knowledge security theory. Having a better understanding of the three concepts, enabled me to take a position in theory through the discussions, definitions, and analysis related to them.

Firstly, regarding organisational knowledge, I outlined the existing definitions of knowledge, from an organisational perspective using a literature review. These were contextualised through the organisational management body of literature and normalised with a tacit and explicit perspective. Following this analysis, I adopted and discussed a definition of organisational knowledge.

Secondly, concerning KM, I aimed to examine the key issues and positions in the literature. I began by examining why KM is important for today’s organisations. Next, I outlined the key theoretical issues and positions in KM. Following this, I discussed the problems that arose when defining KM and aimed to overcome them by arguing for a consolidated definition. Finally, I ended by discussing the key reasons that there is a need to integrate knowledge security with KM. These were then analysed in terms of how such positions create an integrated need for knowledge security.

Thirdly, regarding knowledge security, I reviewed the literature and examine what security approaches are expressed therein, keeping the KM paradigm in mind. I did so by examining why there is a need for knowledge security. Next, I used the literature to categorise and establish the core paradigms and perspectives as they relate to knowledge security. Using this

³⁷ Mouton, 2001. *How to Succeed in your Master and Doctoral Studies: A South African Guide and Resource Book* p 137-142.

as a base, I then proceeded to outline the key perspectives according to their general thematic paradigms. Thus, it helped to set the groundwork for the empirical component to follow and to provide the inputs necessary for the development of the conceptual model.

1.3.2 Empirical Analysis

As knowledge security holds practical implications for organisations, I thought that it is important to connect it to the real world in some capacity. The purpose of this was to have a practical understanding of the relationship between security and KM and to obtain inputs from practice that could be used in the development of the conceptual model. This was examined in terms of how organisations currently deal with knowledge security in practice.

However, as I am dealing with knowledge security, a sensitive subject, it was also felt that access to key comprehensive and comparative data aspects would not be easily obtained, at least in all cases, if organisations were asked directly about their key security practices. For example, it would defeat the purpose of most organisations security policies to share such information in terms of having to maintain confidentiality³⁸. Therefore, in doing so, it runs the risk of obtaining lower quality results. To mitigate this risk, I chose to expand the empirical analysis to also include content, which is open, but still a good representation of what could be going on in organisations. As such, I chose to also focus on analysing the web content of leading academic institutions in the field of information science or studies. This was done under the assumption that how these leading institutions handle the concept of knowledge security would reflect the state of the art as it currently stands in academic training and therefore how it translates into practice. The empirical component of the study was structured in two parts.

The first part of the empirical analysis consisted of a review of whether security and KM are treated as separate entities in the academic programs of leading universities in the field of information science and studies. To do so, I began by firstly outlining how the leading universities were identified. This was followed by an overview of the approach used to examine these leading universities and to establish any relationship to security. Finally, the findings of the analysis were discussed as related to each university and a discussion of the overall findings was given. The approach was premised on the view that what is taught at leading universities in this field would provide an open-source representation of what the state of the art is and thus what is being pursued in organisations. This was based on the initial assumption that security

³⁸ Harris, 2010. *CISSP Certification All-in-One Exam Guide* p 186.

and KM are treated as separate entities in academia and will be treated as separate areas in practice. Subsequently, doing so formed the foundation to confirm or deny the second part of the empirical component of the study and to help provide further inputs for the development of the conceptual model.

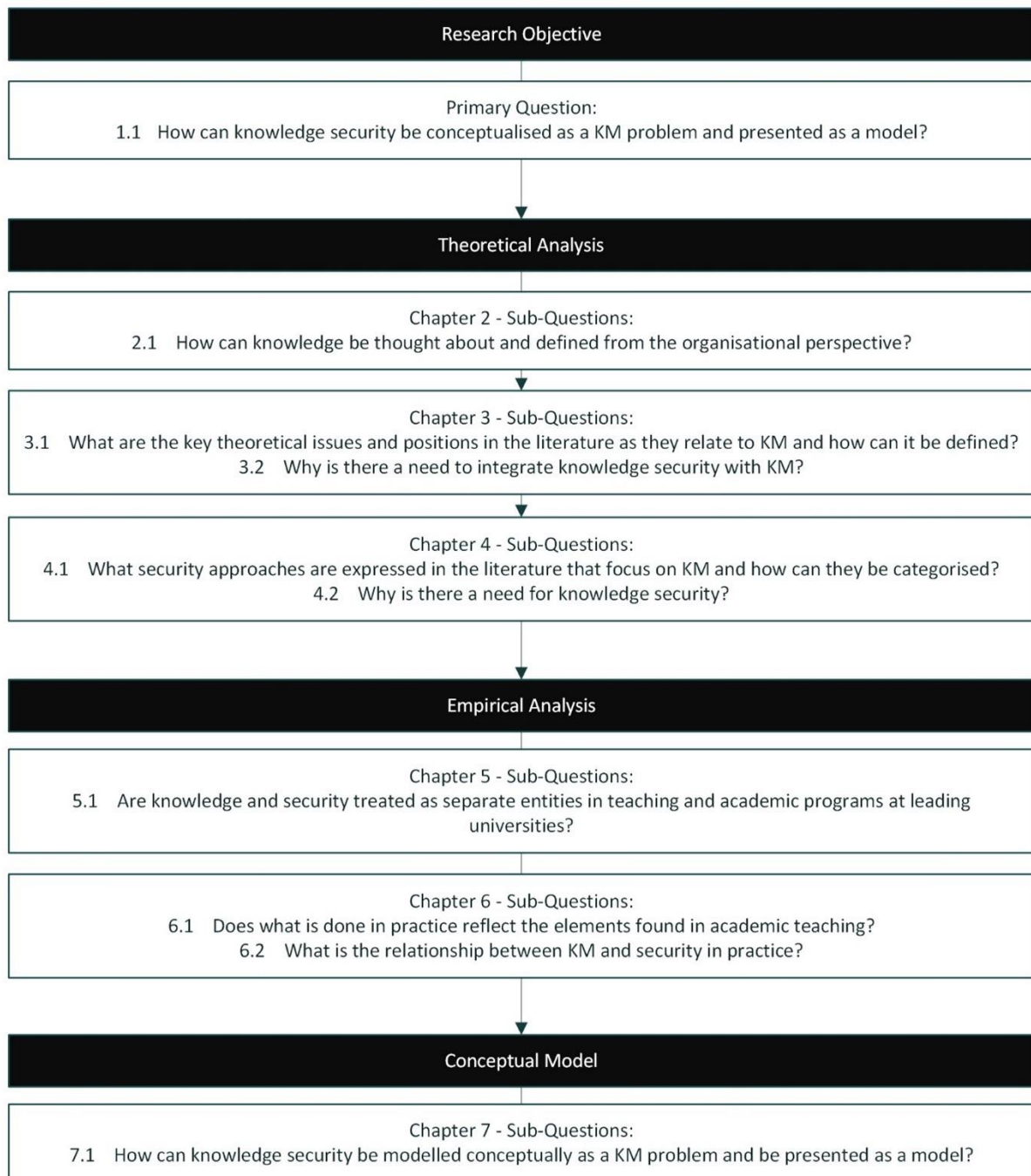
The second part of the empirical analysis aimed to confirm and substantiate these findings. Through the analysis, I aimed to determine if what is done in practice reflects those elements identified in leading academic institutions. To do so, I used a qualitative, interpretive research approach which consisted of a series of semi-structured interviews with nine industry experts. This resulted in the output of eight case study narratives. The findings from the case study narratives helped to contribute to obtaining a practical perspective of KM and its relationship with security. Additionally, they also helped to provide further inputs for the development of the conceptual model.

1.4 The Importance of the Study

There is currently limited research concerning how to secure organisational knowledge systemically and how this can be leveraged in an integrated manner. If knowledge is managed but not protected effectively, an organisation's ability to obtain the full benefit of this resource will be hindered as that resource will be at risk. The study thus aims to neutralise this risk by clarifying how knowledge security can be applied to organisations concerning KM activities in an integrated, balanced manner. This helps to provide clarity and lays the foundation for future research that can contribute to solidifying knowledge security as part of KM processes.

1.5 Chapter Layout

The chapter layout has been derived with the research statement, questions, and study objectives in mind. I have outlined the structure of the study in Figure 1-2, which illustrates how these components fit together. Additionally, a short description of Chapters 2-7 is also given following Figure 1-2.

Figure 1-2: Structure of the Study

Chapter 2 – Outlines the existing definitions of knowledge as a concept, from an organisational perspective, using a literature review. Following this discussion, a definition of organisational knowledge is adopted and discussed.

Chapter 3 – Consists of a review of the key issues and positions in the literature as they relate to KM and how they can be defined in the form of a consolidated definition. The chapter ends by discussing the key reasons as to why there is a need to integrate knowledge security with KM.

Chapter 4 – Reviews the security literature and examines what knowledge security approaches are expressed therein and why there is a need for knowledge security. This is done to establish the core paradigms and perspectives as they relate to knowledge security.

Chapter 5 – Deals with the first part of the empirical component of the study following an open-access approach. It consists of a review of whether knowledge and security are treated as separate entities in the teaching and academic programs of leading universities in the field of information science and studies.

Chapter 6 – Forms the second, and final, part of the empirical component. It outlines the research process and findings related to Chapter 5. It also helps to obtain a practical perspective by reporting on the results of the series of interviews conducted with the nine industry experts.

Chapter 7 – Forms the final part of the research and discusses the process of conceptualising knowledge security as a KM problem, and presenting it as a model. Following this, the limitations of the model are briefly discussed and ideas for further research are presented.

Part 1 – Theoretical Analysis

Chapter 2

Defining Organisational Knowledge

2.1 Introduction

The chapter outlines the existing definitions of knowledge as a concept, from an organisational perspective, using a literature review. The discussion is contextualised through the organisational management parent body of literature. The key definitions of knowledge through the ages are presented and then normalised using a tacit and explicit point of view as a common leveller. Following this discussion, a definition of organisational knowledge is adopted and discussed. This is a precursory measure to overcome the agnostic limitations of Becerra-Fernandez and Sabherwal's KM framework as discussed in Chapter 1.

2.2 Core Definitions of Knowledge

Understanding how knowledge flows through an organisation is vital for innovation and thus competitive advantage, as presented in organisational management theory³⁹. The processes and tools used to manage knowledge in organisations, whether officially called KM or another term⁴⁰, are important contributing factors for organisational success⁴¹. This view is based on the key concepts of sharing, learning, and innovating where knowledge is viewed as the principal source of value creation⁴² in an organisation. In this view, knowledge is embedded and carried through multiple entities including organisational culture, identity, routines, policies, systems, documents, and individuals⁴³. It is based on the perspective that it is framed

³⁹ Gold *et al.*, 2001. *Knowledge Management: An Organisational Capabilities Perspective* p 186.

⁴⁰ Corney, 2013. *Knowledge Management is Dead but it won't lie Down: A 10 Year Review of a KIM Initiative* [Online].

⁴¹ Xu & Quaddus, 2005. *Exploring the Perceptions of Knowledge Management Systems* p 320-334.

⁴² Eardley & Uden (Eds.), 2010. *Innovative Knowledge Management: Concepts for Organisational Creativity and Collaborative Design* p 304.

⁴³ Alavi & Leidner, 1999. *Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues* p 4-6.

through. Knowledge has been considered the main driving force of sustainable competitive advantage⁴⁴ as expressed in business, management, and organisational literature⁴⁵.

However, there is a problem. The way knowledge is managed in organisations, through KM processes, has come to be associated with a significant conceptual drift in its meaning and application⁴⁶. This is predominantly due to the slippery nature of knowledge itself⁴⁷. To better unpack the concept of KM in future chapters and align it with security, a particular definition of organisational knowledge needs to be established. Building upon this definition, an overview of KM literature will set the groundwork for outlining an effective knowledge security model. If this is not done, when dealing with the concept of KM and the KM framework outlined by Becerra-Fernandez and Sabherwal, the conceptual drift will undermine a discussion of knowledge security.

Getting to the core meaning of knowledge is a difficult task, as it is fraught with philosophical complexity^{48 49 50}. From an epistemological framework, knowledge has been defined as ‘justified true belief’⁵¹. However, in attempting to define what knowledge is, Bertrand Russell⁵² outlines that although knowledge may be defined as a true belief, in line with facts, the trouble is that there is little agreement as to what a belief or a fact is⁵³. From his perspective, there is no consensus on the sort of relationship between these concepts that would make a ‘true belief,’ and thus constitute knowledge.

To avoid issues of philosophical complexity, I aim to adopt a recognised practical view of what knowledge means for organisations, as taken from the literature. This approach is necessary, as debating the *true* philosophical meaning of knowledge is not one of the objectives of this

⁴⁴ Alavi & Leidner, 1999. *Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues* p 3.

⁴⁵ Department of Defence. 1999. *Review of the Literature* [Online].

⁴⁶ De Long & Seemann, 2000. *Confronting Conceptual Confusion and Conflict in Knowledge Management* p 33.

⁴⁷ Maasdorp, 2001. *Bridging Individual and Organisational Knowledge: The Appeal to Tacit Knowledge in Knowledge Management Theory* p 1. Maasdorp outlines there is also a second contextual problem in terms of how knowledge is understood and actualised through individuals and the processes of the organisation.

⁴⁸ Russell, 2013. *Theory of Knowledge: The 1913 Manuscript* p 155.

⁴⁹ Bhatt, 2001. *Knowledge Management in Organizations: Examining the Interaction Between Technologies, Techniques, and People* p 69.

⁵⁰ Brinkley, 2006. *Defining the Knowledge Economy* p 5.

⁵¹ Ichikawa & Steup, 2017. *The Analysis of Knowledge*.

⁵² Russell, 2013. *Theory of Knowledge: The 1913 Manuscript* p 45-76.

⁵³ Russell, 2013. *Theory of Knowledge: The 1913 Manuscript* p 45-76.

research. I will deal with the concept of knowledge in the following manner: 1) By outlining the prominent definitions of knowledge through the ages. 2) Adopting a relevant definition well fitted to meet the requirements of organisational knowledge. 3) To outline that definition in more detail and to show how the chosen definition responds to other relevant views of knowledge. 4) To provide a clear outline of the complexities involved in choosing that definition. I will therefore begin the process by providing an overview of the most prominent definitions of knowledge as expressed through the ages.

Table 2-1 outlines this summary of knowledge, which offers a taxonomy stretching broadly from the identification of *mythos* and *logos* by the Socratic school, to modern interpretations relating to knowledge as organisational products and processes as presented by Edvinsson and Malone. Table 2-1 has been adapted from the taxonomy of knowledge presented in the work of Kakabadse *et al.*⁵⁴. Kakabadse *et al.* outline that the concept of knowledge implies both development and growth⁵⁵, and they use the taxonomy as a platform in support of their position on knowledge. The taxonomy which they present has been similarly adapted by other authors such as Chen *et al.*⁵⁶ to provide a conceptual framework for understanding knowledge in their research. The taxonomy, therefore, offers a good overview of the main views of the embodiment of knowledge, without going into excessive detail, and its meaning to different generations from an individual and collective perspective. This taxonomy of the definitions of knowledge is comprehensive enough to be of meaningful value when deciphering what is meant by organisational knowledge.

2.2.1 Normalising Definitions of Knowledge

Although Table 2-1 represents a succinct list of the key definitions of knowledge through the ages, it is not without fault. The problem lies in the way these definitions are presented. They range broadly from definitions of knowledge offered from the times before Christ up to the present day, the scope of which have emerged from vastly different contexts. For example, some of the definitions relate to how knowledge can be viewed as existing in organisations, the collective⁵⁷, while others relate to the philosophical dimensions of knowledge concerning the individual. The latter is somewhat abstract from the organisational context, thus in terms of

⁵⁴ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁵⁵ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁵⁶ Chen *et al.*, 2009. *The Third Category of Knowledge: Concept and Framework* p 4609.

⁵⁷ Alavi & Leidner as cited in Hemsley & Mason, 2013. *Knowledge and Knowledge Management in the Social Media Age*, p 138-167.

Table 2-1: Taxonomies of Knowledge

Authors	Types / Forms of Knowledge and Level of Embodiments
Socrates (Plato, 1953)	<ul style="list-style-type: none"> • Mythos refers to that part of “knowledge” that is arguable and can be demonstrated and identified with precision and agreement – it is extremely personal • Logos derives from gathering, reading, and coming to connote counting, reckoning, explanation, rules, or principles and, finally, reasons. Although mythos and logos represent two realms that constitute knowledge, they are also complementary and interactive poles of knowledge
Bacon (1605)	<ul style="list-style-type: none"> • “Pure knowledge of nature and universality, knowledge by the light where of man did give names unto other creatures in paradise...” • “Proud knowledge of good and evil, which give intent in man to give law unto himself...”
Boswell (1979)	<ul style="list-style-type: none"> • “We know a subject ourselves”; or • “We know where we can find information about it.”
Polanyi (1958, 1996)	<ul style="list-style-type: none"> • Tacit knowledge: Awareness of things that we may not be able to tell; all knowledge is either tacit or rooted in tacit knowledge • Explicit knowledge: Capable of being clearly stated
Schank and Abelson (1977)	<ul style="list-style-type: none"> • General knowledge: Information about, and interpretation of, human intention, disposition, and relationships (satisfaction, enjoyment, achievement, preservation, crisis, instrumental) and “themes” (role themes, interpersonal themes, and life themes) • Specific knowledge: A “script”, a representation of the expected sequential flow of events in a particular situation (cooking, applying for a job) • Expert knowledge: “Factual knowledge” (extensive database about life matters) and “procedural knowledge” (mental procedures, heuristics)
Frantzich (1983)	<ul style="list-style-type: none"> • Resident knowledge: Insider knowledge residing within networks and gatekeepers • Access knowledge: Readily transferable information
Anderson (1985)	<ul style="list-style-type: none"> • Declarative knowledge: Describing something • Procedural knowledge: How something occurs or is performed • Causal knowledge: Why something occurs
Holliday and Chandler (1986)	<ul style="list-style-type: none"> • Knowledge as a general competence: A dimension that overlaps with local intelligence or technical ability • Pragmatic knowledge: Based on experience • Knowledge as a set of reflective or evaluative meta-analytical skills and abilities
Blackler (1993)	<ul style="list-style-type: none"> • Embrained knowledge: Conceptual skills and abilities • Embodied knowledge: Acquired by doing • Encultured knowledge: Acquired through socialization • Embedded knowledge: Organisational routines • Encoded knowledge: Signs and symbols
Nonaka and Takeuchi (1995)	<ul style="list-style-type: none"> • Technical knowledge: “Know-how” • Cognitive knowledge: “Mental models”

Authors	Types / Forms of Knowledge and Level of Embodiments
Heron (1996)	<ul style="list-style-type: none"> • Propositional knowledge: Theoretical ideas about things • Practical knowledge: Action related know-how • Experiential knowledge: Things as actually experienced • Presentational knowledge: A feedback loop from experiential to propositional knowledge in a form of a creative output
Tsoukas (1996)	<ul style="list-style-type: none"> • “Taxonomic” knowledge: Knowledge that makes the distinction between explicit and tacit knowledge
Edvinsson and Malone (1997)	<ul style="list-style-type: none"> • Product knowledge • Routine knowledge • Process knowledge

their relation to one another, when viewed from the confines of the organisation, they lack uniformity. Without a uniform frame of reference to analyse these definitions relationally, on common grounds, understanding them in terms of their applicability in organisational and management contexts becomes difficult.

To overcome this problem, I propose finding a common framework relating to the definitions and analysing them in terms of their relationship to this framework. The objective will be to normalise the definitions into commonly understood themes based upon comparable characteristics. Upon examining the relationship of these themes, to the needs of the organisation from a KM and security perspective, the selection of a definition of knowledge will be possible. Doing so will present a definition that is most relevant to the organisational context. Additionally, this must be done without overlooking definitions of knowledge from some of the more abstract contexts put forward.

Keeping this approach in mind, upon examination of the historical progression and various emphases placed on the nature of knowledge, as outlined in Table 2-1, it becomes clear that two broad themes in the taxonomy of knowledge appear. These themes are namely the concept of knowledge as existing in either a tacit or explicit form⁵⁸. Normalising different views of knowledge in this way is effective because, as Joia and Lemos state, “all knowledge has a tacit and explicit component”⁵⁹. By normalising the definitions of the nature of knowledge along these lines, there is a common point of departure from which to evaluate the definitions based on the same essential elements. In turn, it allows for much more effective adoption, analysis,

⁵⁸ Joia & Lemos, 2010. *Relevant Factors for Tacit Knowledge Transfer within Organisations* p 411.

⁵⁹ Joia & Lemos, 2010. *Relevant Factors for Tacit Knowledge Transfer within Organisations* p 411.

and application of a definition of knowledge within the Becerra-Fernandez and Sabherwal KM framework⁶⁰, and when developing the knowledge security model in subsequent chapters.

2.2.2 A Tacit and Explicit View of Knowledge Definitions

In the light of the definitions presented in Table 2-1, the first clear theme that arises is tacit knowledge. In its purest sense, tacit knowledge is the view of knowledge as something arising from an internalised, personal perspective or process⁶¹ which is outlined in the following extract.

Tacit knowledge is automatic, requires little or no time or thought and helps determine how organisations make decisions and influence the collective behaviour of their members (Liebowitz and Beckman, 1998)... Polanyi (1967) described tacit knowledge as knowing how to do something without thinking about it, like riding a bicycle. This highly personal, subjective form of knowledge is usually informal and can be inferred from the statements of others (Sternbherg, 1997)⁶².

From an organisational perspective, this usually means knowledge that exists within the minds of employees, a firm's intellectual capital, attained as a direct result of experience, reflection, and dialogue⁶³. A firm's approach to the application of tacit knowledge is primarily derived through the context of the organisation, in other words, the socialisation processes that take place, mixed with an employee's previous experiences⁶⁴. Each of these elements can have far-reaching implications for organisations, when viewed from a management framework⁶⁵, in terms of applying this knowledge to create value for the firm.

The second theme that becomes apparent from the progression outlined in Table 2-1 is the idea that knowledge can be derived from an external, formalised, and systematic context. This is what Polanyi calls explicit knowledge, knowledge that is capable of being clearly stated⁶⁶, usually in a codified form. Smith points out that, from the perspective of organisations, the type

⁶⁰ Jasimuddin, 2005. *The Paradox of Using Tacit and Explicit Knowledge: Strategies to Face Dilemmas* p 102.

⁶¹ Nonaka & Toyama, 2003. *The Knowledge-Creating Theory Revisited: Knowledge Creation as a Synthesizing Process* p 5-6.

⁶² Smith, 2001. *The Role of Tacit and Explicit Knowledge in the Workplace* p 314.

⁶³ Joia & Lemos, 2010. *Relevant Factors for Tacit Knowledge Transfer within Organisations* p 411.

⁶⁴ Pathirage *et al.*, 2007. *Tacit Knowledge and Organisational Performance: Construction Industry Perspective* p 115.

⁶⁵ Jasimuddin, 2005. *The Paradox of Using Tacit and Explicit Knowledge: Strategies to Face Dilemmas* p 102.

⁶⁶ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

of knowledge that is seen as explicit knowledge is systemic, codified, and reusable. This type of knowledge exists predominantly outside of the minds of employees.

Most explicit knowledge is technical or academic data or information that is described in formal language, like manuals, mathematical expressions, copyright, and patents. This "know-what" or systematic knowledge is readily communicated and shared through print, electronic methods, and other formal means... Explicit knowledge is carefully codified... explicit knowledge assets can be reused to solve many similar types of problems or connect people with valuable, reusable knowledge⁶⁷.

As the above extract indicates, explicit knowledge does not exist completely separately from tacit knowledge. Rather, the two forms of knowledge exist in parallel with one another, with intersections taking place between the two at critical points of knowledge transfer. Polanyi contends that tacit and explicit knowledge are not sharply divided⁶⁸. While tacit knowledge can exist in isolation, explicit knowledge must be understood tacitly and applied to a context. Considering this, all knowledge is rooted in tacit knowledge to some degree⁶⁹. This perspective is further elaborated by Tsoukas and Mylonopoulos where they argue that social interaction predominantly dictates the type and form that knowledge will take⁷⁰ in organisations. An example of this is outlined by Tsoukas and Mylonopoulos, whereby they highlight that explicit knowledge⁷¹ is combined with the important social aspect of tacit knowledge. In this sense, knowledge is not separated from the social context. Rather, it is seen as resulting from the social interaction that takes place in organisations.

While studying the links between organizational knowledge, learning and capabilities has been the focus of several studies (Chandler, Hagstrom and Solvell, 1998; Choo and Bontis, 2002; Dosi, Teece and Chytry, 1998; Eisenhardt and Santos, 2002; Moingeon and Edmondson, 1996), accounting for how organizational knowledge is established in the first place remains relatively unexplored. It is one thing to take knowledge for granted and then show how it is related to learning and dynamic capabilities (an important task, no doubt), and quite another to explore

⁶⁷ Smith, 2001. *The Role of Tacit and Explicit Knowledge in the Workplace* p 115.

⁶⁸ Polanyi, 1966. *The Logic of Tacit Inference* p 7.

⁶⁹ Polanyi, 1966. *The Logic of Tacit Inference* p 7.

⁷⁰ Tsoukas & Mylonopoulos, 2004. *Introduction: Knowledge Construction and Creation in Organizations* p 4.

⁷¹ Zack, M. 1999. *Managing Codified Knowledge* p 46-48.

questions regarding the social practices in organizations through which what is regarded as ‘knowledge’ attains this status, with what effects⁷².

The definitions of tacit and explicit knowledge provided here are brief in their approach, and it is important to keep in mind that, as with most knowledge-related areas, tacit and explicit knowledge are topics that can be debated in detail. However, for this study, a broad view of tacit and explicit knowledge is adequate to meet the normalisation requirements of the project. Using tacit and explicit knowledge as part of the normalisation process should be considered a stepping-stone on the way to adopting a new perspective of knowledge in the organisational context. It is important to remember, that the adopted definition of knowledge will be expanded in discussing the intersection of tacit and explicit knowledge in greater detail. The definitions of knowledge will be analysed broadly to establish their relationships to the definitions of tacit and explicit knowledge expressed in this section.

2.2.3 Normalising Knowledge Definitions Through a Tacit and Explicit Framework

Defining knowledge was a central subject of philosophy and epistemology during the time of the ancient Greeks⁷³. Although imperfect in terms of the logic of the definitions offered by the ancient Greeks⁷⁴, their definitions continue to have a prominent influence on views of knowledge⁷⁵ in Western Philosophy⁷⁶. As highlighted in Table 2-1, some of the earliest attempts by the Greeks to define knowledge emerged from the Socratic school of thought. Here, reference was made to knowledge as *mythos*, which can be defined as a personal view of knowledge existing from within the self⁷⁷. This builds upon Plato’s view that knowledge is “justified true belief”⁷⁸, as described in his *Meno*, *Phaedo* and *Theaetetus*⁷⁹. Emphasising the view that knowledge exists from within the self holds true for a tacit view of *mythos*, as

⁷² Tsoukas & Mylonopoulos, 2004. *Introduction: Knowledge Construction and Creation in Organizations* p 2.

⁷³ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 77.

⁷⁴ Nonaka & Takeuchi, 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* p 60.

⁷⁵ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 77.

⁷⁶ Nonaka & Takeuchi, 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* p 60.

⁷⁷ Shelburne, 1988. *Mythos and Logos in the Thought of Carl Jung: The Theory of Collective Unconscious in Scientific Perspective* p 107-108.

⁷⁸ Plato cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 76.

⁷⁹ Plato cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 76.

internalised knowledge associated with the individual is a key element of tacit approaches⁸⁰. By framing *mythos* from this perspective, parallels can also be drawn to the tacit dimension of individualistic knowledge in organisations, and how that might relate to explicit perceptions when carrying out tasks.

From an explicit knowledge view, the Socratic school's view of *logos* can be seen to describe many of the characteristics of explicit knowledge. Fine outlines Plato's *logos* condition of knowledge as concerned with the content of one's claim to know⁸¹. Plato states, according to Fine, that *logos* must be suitably explanatory, "if my definition of *x* is in terms of *y* and *z*... Knowledge, Plato believes, must be based on knowledge"⁸². This hints at the interaction and reliance of explicit forms of knowledge upon tacit knowledge for their context, application and meaning. *Logos* may not be expressively explicit, but from the standpoint of tacit and explicit interaction, it mirrors many of the important factors of perception and context found in organisations⁸³, particularly when dealing with the meaning and application of knowledge.

Bacon and Boswell also support such a perspective, by emphasising the creation of knowledge as an activity that is based heavily on the projection of personalised thoughts and ideas. For example, Bacon states "man did give names unto other creatures in paradise"⁸⁴ and Boswell states "we know a subject ourselves"⁸⁵. These excerpts imply a dependence upon an individual's interpretation, perception, and application of internalised processed knowledge. Framed from a tacit understanding of knowledge, these views make sense in terms of how an individual incorporates and applies knowledge but makes little mention of the need for socialisation as a catalyst for doing so.

However, these views are aligned with an understanding of the impact of the natural environment as a conduit that enables the intersection of human power and knowledge⁸⁶. By taking such a stance, a traditional view of socialisation for knowledge generation is mitigated in favour of a contextual one. From Bacon's perspective, this is seen as a critical factor for the

⁸⁰ Smith, 2001. *The Role of Tacit and Explicit Knowledge in the Workplace* p 314.

⁸¹ Fine, 1979. *Knowledge and Logos in the Theaetetus* p 367.

⁸² Fine, 1979. *Knowledge and Logos in the Theaetetus* p 367.

⁸³ Gero, 1990. *Design Prototypes: A Knowledge Representation Schema for Design* p 26.

⁸⁴ Bacon cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁸⁵ Boswell cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁸⁶ Bacon, 2014. *The New Organon* p 1-7.

valid creation and manifestation of knowledge in the individual⁸⁷. Bacon focuses his attention more so on the tacit dimension of knowledge and its use, without leveraging what could be considered the explicit dimension in his definition.

However, Boswell offers an interesting definition of knowledge wherein the author alludes to both the tacit, and to some degree the explicit dimensions of knowledge, but without directly contrasting the two. By defining knowledge with examples such as “we know a subject ourselves”⁸⁸ or “we know where we can find information about it”⁸⁹, it is implied that there is some feedback and exchange taking place between tacit and explicit forms of knowledge. This is implied firstly in the way we interpret and integrate such knowledge into our frame of reference, the tacit dimension, through a need to “find information about it”⁹⁰ and the need to explore and integrate codified knowledge within the self; “we know a subject ourselves”⁹¹. By stating “find information about it... we know a subject ourselves”⁹², Boswell indirectly alludes to the existence of explicit forms of knowledge, manifested through the tacit requirements of the individual brought about by contextual challenges.

What could be considered the first modern definition of tacit knowledge comes from Polanyi, who was the first to name knowledge as tacit and explicit⁹³. From Polanyi’s perspective, tacit knowledge relates to an understanding of the fiduciary element of the intrinsic belief that exists within people⁹⁴; this whereby Polanyi defines tacit knowledge as an “awareness of things that we may not be able to tell”⁹⁵. The process of tacit knowledge creation, from Polanyi’s perspective, thus relies upon each person’s interpretation of external cues governed by their perception⁹⁶. In this instance, a person’s perception acts as a filter through which certain feeds

⁸⁷ Bacon, 2014. *The New Organon* p 1-7.

⁸⁸ Boswell cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁸⁹ Boswell cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁹⁰ Boswell cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁹¹ Boswell cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁹² Boswell cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁹³ Ambrosini & Bowman, 2001. *Tacit Knowledge: Some Suggestions for Operationalization* p 812.

⁹⁴ Polanyi, 2015. *Personal Knowledge: Towards a Post-Critical Philosophy* p x.

⁹⁵ Polanyi cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

⁹⁶ Conover & Feldman, 1984. *How People Organize the Political World: A Schematic Model* p 96.

pass, the ways of looking and perceiving things from the external world and are in turn inducted into their psyche in the form of beliefs⁹⁷. The induction process shapes a person's perception and further alters the filter through which their external feeds are processed, becoming part of their psyche and belief system accordingly. Thus, it can be explained in the form of personal schemas, a person's experience, and expertise, which shape preconceptions of an individual's tacit knowledge and modify it in future interactions. It should be noted that such schemas cannot be applied or evaluated from a knowledge perspective if they are devoid of context or socialisation.

This paradigmatic shift in perspectives has led psychologists to focus more on how knowledge is stored and how such stored information subsequently influences the perceptual process. In such efforts, the concept of a "schema" has played a central role... A schema may be defined as a cognitive structure of "organised prior knowledge, abstracted from experience with specific instances" that guides "the processing of new information and the retrieval of stored information" ... For example, a schema of the role of "candidate" might include very general beliefs about the goals of candidates along with more specific information about the particular activities that candidates engage in to get elected⁹⁸.

As per Polanyi's definition in Table 2-1, explicit knowledge is that which is "capable of being clearly stated"⁹⁹. Polanyi contextualises tacit knowledge in relation to explicit knowledge as situated around the workings of an individual's cognitive processes. For example, Polanyi states "let us recognise that tacit knowledge is the fundamental power of the mind which creates explicit knowing, lends meaning to it and controls its uses"¹⁰⁰. This is not to say that Polanyi follows a behaviouristic approach; in fact, he firmly rejects this¹⁰¹. Rather, Polanyi makes a case for exploring the concept of knowledge as something which does not require the over-purification of science¹⁰² but does require the interaction of tacit and explicit forms of knowledge to take place to generate new knowledge.

⁹⁷ Conover & Feldman, 1984. *How People Organize the Political World: A Schematic Model* p 96-98.

⁹⁸ Conover & Feldman, 1984. *How People Organize the Political World: A Schematic Model* p 96.

⁹⁹ Polanyi cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹⁰⁰ Polanyi, 1966. *The Logic of Tacit Inference* p 18.

¹⁰¹ Polanyi, 1966. *The Logic of Tacit Inference* p 14.

¹⁰² Polanyi, 1966. *The Logic of Tacit Inference* p 18.

Schank and Abelson's definition of knowledge reflects the convergence of psychology and artificial intelligence (AI) as an approach used to frame the nature of knowledge¹⁰³. Their view using terms such as "general knowledge", "specific knowledge" and "expert knowledge"¹⁰⁴ lends itself strongly towards a tacit understanding of knowledge rather than an explicit one. The taxonomy that they have used implies a view of knowledge that exists not only within the individual from a pragmatic developmental standpoint¹⁰⁵. It is also one that is dependent upon the processes, networks and social contexts for the development, interpretation and framing of knowledge¹⁰⁶.

Frantzich builds upon this definition of knowledge, in the first part of his definition, which echoes a tacit knowledge view by categorising knowledge as "resident knowledge"¹⁰⁷. Resident knowledge is explained by Frantzich as insider knowledge residing within networks and the gatekeepers within those networks¹⁰⁸. Frantzich's metaphor of a network with interconnecting nodes to describe knowledge comes from his background in political science and IT¹⁰⁹. These he uses in combination to describe and analyse knowledge¹¹⁰. As special attention is given to the importance of insider knowledge, which lends itself to a tacit view of knowledge, the implications of knowledge networks in politics rely heavily on the importance of individual knowledge. From Frantzich's perspective, this approach is critical for successfully navigating the concept of knowledge in diverse political and informational contexts.

The second part of Frantzich's definition represents an explicit view of knowledge. From this view, Frantzich's definition refers in part to what he calls "access knowledge"¹¹¹. Frantzich outlines access knowledge as that which has been encoded in the form of information¹¹² and is

¹⁰³ Schank & Abelson, 1977. *Scripts, Plans, Goals and Understanding: An Inquiry into Human Knowledge Structures* p 190.

¹⁰⁴ Schank and Abelson cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹⁰⁵ Schank & Abelson, 1977. *Scripts, Plans, Goals and Understanding: An Inquiry into Human Knowledge Structures* p 191.

¹⁰⁶ Schank & Abelson, 1977. *Scripts, Plans, Goals and Understanding: An Inquiry into Human Knowledge Structures* p 191-199

¹⁰⁷ Frantzich cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹⁰⁸ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹⁰⁹ Chen *et al.*, 2009. *The Third Category of Knowledge: Concept and Framework* p 4609.

¹¹⁰ Chen *et al.*, 2009. *The Third Category of Knowledge: Concept and Framework* p 4609.

¹¹¹ Frantzich cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹¹² Bellinger *et al.*, 2004. *Systems Thinking: Data, Information, Knowledge, and Wisdom*.

thus readily transferable¹¹³. This definition which refers to knowledge as an encoded form of information, something that can be reused and shared multiple times, falls within the definitions and examples of explicit knowledge.

Anderson attempts to categorise knowledge from a predominantly tacit perspective. He does this in three primary ways: 1) As declarative, or descriptive knowledge. 2) As procedural or knowing how something occurs or is performed. 3) As causal or knowing why something occurs¹¹⁴. These views of knowledge highlight the importance of the individual's ability to process knowledge, and gain meaning based on the cues derived from their environment, through routines and processes. As expressed in the earlier definition of tacit knowledge, this is a key characteristic. In addition, the individual is central in Anderson's view of knowledge. This is expressed in his definitions of knowledge, where he uses words like "descriptive knowledge... knowing how something occurs... knowing why something occurs"¹¹⁵. The meanings derived from these words fall directly within the context of tacit definitions of knowledge, as they revolve around knowing something rather than relying upon insight from the codified forms of knowledge. Anderson does not explicitly mention socialisation as a contributing factor to knowledge generation, however, the role of the environment's influence is implied by his references to "application situation"¹¹⁶. This point is illustrated in a later paper by Anderson *et al.* when discussing knowledge acquisition.

In general, we argue that the goals of advanced knowledge acquisition in complex and ill-structured domains can best be attained... by the development of mental representations that support cognitive flexibility... foster the ability to assemble diverse knowledge sources to adaptively fit the needs of a particular knowledge application situation (rather than the search for a precompiled schema that fits the situation)¹¹⁷.

Holliday and Chandler define the concept of knowledge from a slightly different framework, with this framework remaining largely tacit based in its approach. They position their view of the nature of knowledge from within the paradigm of evaluating the meaning of wisdom. They

¹¹³ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹¹⁴ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹¹⁵ Anderson cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹¹⁶ Anderson cited in Spiro *et al.*, 1988. *Cognitive Flexibility Theory: Advanced Knowledge Acquisition in Ill-Structured Domains* p 556.

¹¹⁷ Anderson *et al.* cited in Spiro *et al.*, 1988. *Cognitive Flexibility Theory: Advanced Knowledge Acquisition in Ill-Structured Domains* p 556.

do so predominantly in an individualistic and cultural sense through an understanding of the concept of wisdom. As they state, “the first step in achieving some better understanding of the concept of wisdom lies in the direction of determining more precisely how this notion is commonly understood¹¹⁸”. Bearing this view in mind, they outline in Table 2-1 that knowledge can be viewed as a general competence, experience-based, and as something reflective or evaluative of analytical skills and abilities. These ideas fit within the realms of the earlier definition of what could be considered tacit knowledge. The reference is made to knowledge as something that exists by and relies on an individual’s internalised processes, skills, and abilities in the pursuit of wisdom; from a competence and experience-based paradigm.

Blackler outlines that within the literature there are five views of knowledge that can be identified¹¹⁹. These are listed in Table 2-1 as embrained, embodied, encultured, embedded, and encoded knowledge¹²⁰. Of these definitions of knowledge, embrained, encultured and embedded knowledge can lend themselves to a tacit definition of knowledge as they are primarily based on conceptual skills and abilities¹²¹. Embodied knowledge can be viewed as overlapping with both tacit and explicit definitions of knowledge as it not only involves codified information but also sensory perception and abilities¹²².

The first view of knowledge that lends itself to a tacit definition is that of embrained knowledge. Embrained knowledge falls within the realm of what Blackler calls “abstract knowledge”¹²³. Abstract knowledge relates to higher-level abilities in understanding, an ability to develop complex rules and to understand complex causations within the framework of organisational learning¹²⁴. It is an inherently tacit knowledge process. Embodied knowledge is viewed by Blackler as “know-how”¹²⁵ and depends on peoples’ physical presence, sentiment, sensory information, cues and face-to-face discussions. Blackler believes this type of knowledge is acquired by doing, which is rooted in specific contexts¹²⁶. Encultured knowledge

¹¹⁸ Holiday & Chandler cited in Yang, 2001. *Conceptions of Wisdom among Taiwanese Chinese* p 664.

¹¹⁹ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1023.

¹²⁰ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹²¹ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹²² Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹²³ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1023.

¹²⁴ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1023.

¹²⁵ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹²⁶ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

“refers to the process of achieving shared understandings”¹²⁷. According to Blackler, this is achieved through the cultural meaning of systems that are intimately related to the processes of socialisation and are open to negotiation¹²⁸. Encultured knowledge fits within the definition of tacit knowledge as it is achieved through processes of socialisation. Embedded knowledge is heavily dependent upon an individual’s skills concerning their organisational environment¹²⁹. This environment is made up of a complex mix of processes, systems, routines, interpersonal, technological, and socio-structural factors¹³⁰. These are fundamental processes associated with tacit knowledge generation. Knowledge of how to successfully navigate this environment is embedded within an organisation’s routines and interactions, in the form of “architectural knowledge”¹³¹, which is often taken for granted¹³².

Blackler also views knowledge from a systems perspective with the use of the terms ‘embodied’ and ‘encoded’ knowledge relating to definitions of knowledge as explicit. However, it should be noted, as Blackler states in a later paper on the forms of knowledge, “embodied knowledge is only partly explicit”¹³³. Due to this, Blackler focuses more on encoded knowledge as being truly explicit. Blackler states that encoded knowledge is information conveyed by signs and symbols: “To the traditional forms of encoded knowledge, such as books, manuals and codes of practice, has been added to information encoded and transited electronically”¹³⁴. From this view, knowledge has been codified in informational materials and as such has become explicit. It should be noted, however, that in Blackler’s later work he makes a case against following an approach of viewing knowledge-intensive firms as dealing simply with embodied, embedded, embrained, encultured and encoded forms of knowledge¹³⁵. Rather, Blackler claims that organisations should view knowledge as being the result of the culturally located systems and processes through which people interact and thereby generate their knowledge. Blackler’s argument is outlined in the following extract.

¹²⁷ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹²⁸ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹²⁹ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹³⁰ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹³¹ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹³² Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹³³ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹³⁴ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹³⁵ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1021.

Knowledge (or, more appropriately, knowing) is analysed as an active process that is mediated, situated, provisional, pragmatic, and contested. Rather than documenting the types of knowledge that capitalism currently demands the approach suggests that attention should be focused on the (culturally located) systems through which people achieve their knowledge, on the changes that are occurring within such systems, and on the processes through which new knowledge may be generated¹³⁶.

Nonaka and Takeuchi on the other hand view knowledge as existing as either technical “know-how” or in the form of cognitive “mental models”¹³⁷ inside the minds of the individuals within an organisation. Broda outlines that Nonaka and Takeuchi aim to distinguish between the cognitive and technical elements of tacit knowledge¹³⁸. Nonaka and Takeuchi state that cognitive elements include things like “schemata, paradigms, perspectives, beliefs, and viewpoints which help individuals to perceive and define their world”¹³⁹. The technical elements are made up of “concrete know-how, crafts and skills”¹⁴⁰. Broda elaborates that tacit knowledge tends to include knowledge gained through experience, while explicit knowledge tends to contain knowledge gained through rational thinking¹⁴¹. The predominant positioning of Nonaka and Takeuchi’s view of knowledge in organisations is primarily based upon the use and transfer of tacit knowledge¹⁴² to tacit and explicit forms. This is done to create innovation in organisations to compensate for the uncertainty¹⁴³ created by the global business environment; a result of the information age¹⁴⁴.

Heron aims to define knowledge as constituting four key forms, namely: propositional – theoretical ideas about things; practical – action related know-how; experiential – things as actually experienced; and presentational – a feedback loop from experiential to propositional

¹³⁶ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1021.

¹³⁷ Nonaka & Takeuchi cited in Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹³⁸ Broda, 2005. *Intercultural Challenges of Knowledge Focus Strategy Implementation in China* p 4-51.

¹³⁹ Nonaka & Takeuchi, 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* p 60.

¹⁴⁰ Nonaka & Takeuchi, 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* p 60.

¹⁴¹ Broda, 2005. *Intercultural Challenges of Knowledge Focus Strategy Implementation in China* p 4-51.

¹⁴² Kwek, 1995. *Review: The Knowledge-Creating Company* p 2-3.

¹⁴³ Kwek, 1995. *Review: The Knowledge-Creating Company* p 2-3.

¹⁴⁴ Shear, 2009. *Business Counterintelligence: Sustainable Practice or Passing Fad?* p 32-50.

knowledge as a form of creative output¹⁴⁵. Heron's view of knowledge holds true for the tacit definition of knowledge, as it relies upon paradigms. This is an inherently internalised approach, dependent upon socialisation and context for interpreting meaning. Some components of Heron's explanation, those that relate to presentational knowledge, could be considered explicit in the sense that he states that our "resonance with the imagining of our world... is symbolised"¹⁴⁶ in various art forms. This symbolisation, although holding some explicit truth, falls short of aligning with the explicit definition of knowledge as it is not about codifying knowledge. It is about the process of encapsulating artistic emotion as an artistic artefact. The artistic artefact is a representation of the abstract, presented in a metaphorical form. Heron argues that this view of knowledge constitutes a participatory worldview that accounts for experiential knowing using these paradigms¹⁴⁷. Heron's explanation of this process, and what a participatory worldview means, in terms of knowledge, is outlined in the following extract.

For there is the important if obvious point that knowers can only be knowers when known by other knowers. Knowing presupposes mutual participative awareness... Experiential knowing thus articulates reality through inner resonance with what there is and through perceptually enacting... Its forms of appearing... Presentational knowing... is evident in an intuitive grasp of the significance of our resonance with the imagining of our world as this grasp is symbolised in graphic, plastic, musical, vocal, and verbal art forms. It clothes our experiential knowing of the world in the metaphors of aesthetic creation... Propositional knowing is knowing in conceptual terms that something is the case; knowledge by description... statements and theories... Practical knowing is knowing how to do something, demonstrated in a skill or competence¹⁴⁸.

Tsoukas frames knowledge from both a tacit and explicit perspective. He does this based on a taxonomic perspective of knowledge¹⁴⁹, whereby "the taxonomy of the knowledge elements becomes a core aspect"¹⁵⁰ in defining knowledge. This allows Tsoukas to draw attention to the

¹⁴⁵ Heron & Reason, 1997. *A Participatory Inquiry Paradigm* p 280-283.

¹⁴⁶ Heron cited in Heron & Reason, 1997. *A Participatory Inquiry Paradigm* p 275-281.

¹⁴⁷ Tsoukas cited in Heron & Reason, 1997. *A Participatory Inquiry Paradigm* p 274.

¹⁴⁸ Tsoukas cited in Heron & Reason, 1997. *A Participatory Inquiry Paradigm* p 275-281.

¹⁴⁹ Al-Mualla, 2013. *Tacit Knowledge in Organisations – Towards an Empirical Inquiry* p 4.

¹⁵⁰ Cabrera-Suárez *et al.*, 2001. *The Succession Process from a Resource- and Knowledge-Based View of the Family Firm* p 39.

important dependence of knowledge on the context in which it is being applied¹⁵¹. By focusing on the taxonomy of the knowledge elements, Tsoukas also reaffirms the importance of Polanyi's original view that explicit knowledge cannot exist without tacit knowledge¹⁵². In this regard, Tsoukas takes issue with the modern movement of the "de-contextualisation of knowledge"¹⁵³ that has occurred, which he views as having moved too far away from Polanyi's original outline of the role of tacit knowledge¹⁵⁴. Al-Mualla highlights that this is an important point that becomes particularly relevant when trying to decode knowledge in organisational settings¹⁵⁵. Tsoukas' view of how knowledge should be understood, particularly from a tacit perspective, is in line with Polanyi's original arguments¹⁵⁶ and outlined in the following extract by Crane.

Tsoukas' ideas are grounded in the derivative of those theorised by Polanyi... Polanyi offers a detailed and reasoned argument for turning away from the traditional view and practice of the exact sciences – the pursuit of objective knowledge and scientific detachment. Instead, he argues for the importance of the scientist – the 'knower' – in the act of discovery and validation of scientific knowledge. Accordingly, the scientist brings to his scientific practice his own skills, commitment and experiences which must necessarily form part of the science. Using Polanyi's arguments, Tsoukas criticises the modern movement towards the de-contextualisation of knowledge. Arguing for a phenomenological conceptualisation of tacit knowledge, Tsoukas, as does Polanyi, insists that explicit knowledge cannot exist without the tacit. This personal co-efficient factor suggests that "knowing something, then, is always a contextual issue and fundamentally connected to action"¹⁵⁷.

¹⁵¹ Tsoukas cited in Crane, 2013. *A New Taxonomy of Knowledge Management Theory: The Turn to Knowledge as Constituted in Social Action* p 1-20.

¹⁵² Tsoukas cited in Crane, 2013. *A New Taxonomy of Knowledge Management Theory: The Turn to Knowledge as Constituted in Social Action* p 1-20.

¹⁵³ Tsoukas cited in Crane, 2013. *A New Taxonomy of Knowledge Management Theory: The Turn to Knowledge as Constituted in Social Action* p 1-20.

¹⁵⁴ Tsoukas cited in Al-Mualla, 2013. *Tacit Knowledge in Organisations – Towards an Empirical Inquiry* p 5.

¹⁵⁵ Al-Mualla, 2013. *Tacit Knowledge in Organisations – Towards an Empirical Inquiry* p 5.

¹⁵⁶ Tsoukas cited in Joia & Lemos, 2010. *Relevant Factors for Tacit Knowledge Transfer within Organisations* p 411.

¹⁵⁷ Crane, 2013. *A New Taxonomy of Knowledge Management Theory: The Turn to Knowledge as Constituted in Social Action* p 1-20.

Tsoukas and Vladimirou view knowledge as the capability of members of an organisation to draw distinctions in the process of carrying out their work¹⁵⁸. Tsoukas and Vladimirou suggest that this is done by enacting sets of generalisations. The application of these enacted sets of generalisations depends on the historically evolved collective understandings that individuals have internalised¹⁵⁹. In addition to highlighting the contribution Polanyi has made¹⁶⁰, Tsoukas and Vladimirou also argue that most scholars have failed to engage adequately with Polanyi's work. From Tsoukas and Vladimirou's view, scholars are often seen to miss the point that Polanyi highlights concerning the *personal* character of knowledge¹⁶¹. This is explained in more detail in the following extract.

Moreover, it needs to be pointed out that, although no self-respecting researchers have so far failed to acknowledge their debt to Polanyi for the distinction he drew between tacit and explicit knowledge, Polanyi's work, for the most part, has not been really engaged with. If it had been it would have been noticed that, since all knowledge has its tacit presuppositions, tacit knowledge is not something that can be converted into explicit knowledge, as Nonaka and Takeuchi... have claimed... Moreover, and perhaps more crucially, it would have been acknowledged that Polanyi... more than anything else, insisted on the *personal* character of knowledge – hence the title of his magnum opus, *Personal Knowledge*. In his own words: 'All knowing is personal knowing – participation through indwelling'¹⁶².

Finally, Edvinsson and Malone define knowledge from within an intellectual capital framework¹⁶³ which exists under the visible company buildings and products¹⁶⁴. Intellectual capital in this instance is defined as a collection of knowledge, information, intellectual property (IP), and experience¹⁶⁵. From this definition, knowledge can be found within the intellectual capital frame as existing in the form of products, routines, and processes along with

¹⁵⁸ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 973.

¹⁵⁹ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 973.

¹⁶⁰ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 975.

¹⁶¹ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 975.

¹⁶² Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 975.

¹⁶³ Bontis, 2001. *Assessing Knowledge Assets: A Review of the Models Used to Measure Intellectual Capital* p 42.

¹⁶⁴ Edvinsson & Malone, 1997. *Intellectual Capital: Realizing Your Company's True Value by Finding its Hidden Brainpower* p 11.

¹⁶⁵ Bontis, 2001. *Assessing Knowledge Assets: A Review of the Models Used to Measure Intellectual Capital* p 42.

some other forms of intangible assets¹⁶⁶. Taking this view of knowledge lends itself in both tacit and explicit forms. Defining knowledge in the form of routines, processes and intangible phenomena, a hidden element within organisations¹⁶⁷, mirrors many of the characteristics of the tacit definitions of knowledge. While on the other hand, defining knowledge as intellectual capital, a part of which is information, alludes to explicit definitions of knowledge.

Edvinsson and Malone primarily view knowledge as an intangible resource, one that needs to have adapted intellectual capital accounting structures in place to measure its true value for organisations¹⁶⁸. This adapted intellectual capital is coupled with the value derived from knowledge's interconnectedness with the organisational environment¹⁶⁹. Along with interconnectedness, Edvinsson also highlights the importance of the organisational context in understanding the dynamics of knowledge in practice¹⁷⁰. Additionally, how organisations can understand what knowledge means for them through dialogue. This is done to help organisations visualise knowledge assets outside the traditional balance sheet¹⁷¹. Edvinsson sees this as a critically important factor to have in place if one is to better grasp how intellectual capital can be used, particularly in leveraging the strategic value of knowledge for an organisation¹⁷². Both views hint at tacit definitions of knowledge by mentioning its intangible nature, collective understandings through dialogue and reliance on the organisational environment for deriving meaning.

2.2.4 Key Issues of Knowledge from an Organisational Perspective

Normalising the definitions of knowledge outlined in Table 2-1, from a tacit and explicit perspective, helps to reveal key issues of knowledge from an organisational view. These key issues of knowledge are: 1) Context/environment. 2) Social aspects. 3) Knowledge transfer.

¹⁶⁶ Bontis, 2001. *Assessing Knowledge Assets: A Review of the Models Used to Measure Intellectual Capital* p 11.

¹⁶⁷ Bontis, 2001. *Assessing Knowledge Assets: A Review of the Models Used to Measure Intellectual Capital* p 44.

¹⁶⁸ Edvinsson & Malone, 1997. *Intellectual Capital: Realizing Your Company's True Value by Finding its Hidden Brainpower* p 11.

¹⁶⁹ Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 377.

¹⁷⁰ Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 377.

¹⁷¹ Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 379.

¹⁷² Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 379.

Considering these key issues, I will use these highlighted elements to determine which definition of knowledge will be best suited to meet the requirements of organisational knowledge. Consideration will also be given to how well the adopted definition can align itself with KM and security aspects in addition to the key issues from an organisational perspective. As the key issues act as a framework for identifying a relevant and applicable definition of organisational knowledge, I explain each, derived from the outlines of the normalised definitions of knowledge. Since the key issues are associated with the same objective, that of defining organisational knowledge, there will be some overlap. As such, they do not exist in isolation from one another and are instead interrelated.

Firstly, from the perspective of the context/environment issue, knowledge is critically dependent upon the context/environment in which it is being applied. In this case, the environment acts as a conduit through which the intersection of human power and knowledge¹⁷³ takes place. This is a critical factor in the creation and manifestation of knowledge from a tacit, individual view¹⁷⁴, as well as for the creation of explicit forms of knowledge within organisations. These explicit forms of knowledge are manifested through tacit requirements brought about by contextual challenges¹⁷⁵, which the organisational environment requires. Contextual challenges are dealt with in terms of the application of situational factors as a way of generating and using knowledge¹⁷⁶ in such contexts.

This aspect also aligns with the importance that external cues play as a means of governing perception in these contexts. These cues are derived from the external environment by individuals and influence the creation of beliefs and views¹⁷⁷ within the individuals. The beliefs and views are then actualised through socialisation processes and actions. This can be seen in the form of embodied knowledge, which is acquired by socialisation and which remains contextually dependent¹⁷⁸.

The environment also holds relevance for embedded knowledge, whereby it is dependent upon individual skillsets relating to the requirements of the organisational environment¹⁷⁹. The

¹⁷³ Bacon, 2014. *The New Organon* p 1-7.

¹⁷⁴ Bacon, 2014. *The New Organon* p 1-7.

¹⁷⁵ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹⁷⁶ Spiro *et al.*, 1988. *Cognitive Flexibility Theory: Advanced Knowledge Acquisition in Ill-Structured Domains* p 556.

¹⁷⁷ Conover & Feldman, 1984. *How People Organize the Political World: A Schematic Model* p 96.

¹⁷⁸ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹⁷⁹ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

organisational environment in this instance is seen to be made up of a complex mix of processes, systems, routines, interpersonal, technological, and socio-structural factors¹⁸⁰. These are the systems through which knowledge flows. Knowledge of how to navigate the organisational environment is thus submerged within an organisation's routines and interactions in the form of "architectural knowledge"¹⁸¹, which is generally taken for granted by individuals¹⁸². The influence of the environment on how knowledge is viewed and used in organisations is also relevant to how organisations respond to external uncertainty.

Uncertainty, and the need to respond to it, comes about due to the shifting nature of the global business environment. Organisations try to leverage these uncertainties for their benefit through knowledge processes, in the pursuit of innovation¹⁸³. They do so to ultimately use this innovation to achieve strategic advantage through the interconnected processes of the organisational environment¹⁸⁴ and in response to the global business environment. As such, the environment creates meaning for the organisation¹⁸⁵ and meaning for the organisation's internal processes¹⁸⁶ as perceived by its individuals. Knowledge thus has an important dependence upon the context and environment in which it is being applied¹⁸⁷.

Secondly, from the issue of social interaction, organisational knowledge is considered dependent upon social interactions for its creation, use and the meaning it holds for how knowledge is framed within organisations¹⁸⁸. Knowledge, therefore, relies upon the individual paradigms of those who make up the organisation, and these individual paradigms are in turn dependent upon socialisation and context to garnish meaning¹⁸⁹, interpreted by the individual. This process is not carried out by individuals in isolation, but rather through the collective interactions they experience. These interactions can be in the form of discussions, sentiment or

¹⁸⁰ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹⁸¹ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹⁸² Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹⁸³ Kwek, 1995. *Review: The Knowledge-Creating Company* p 2-3.

¹⁸⁴ Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 377.

¹⁸⁵ Heron & Reason, 1997. *A Participatory Inquiry Paradigm* p 275-281.

¹⁸⁶ Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 379.

¹⁸⁷ Crane, 2013. *A New Taxonomy of Knowledge Management Theory: The Turn to Knowledge as Constituted in Social Action* p 1-20.

¹⁸⁸ Schank & Abelson, 1977. *Scripts, Plans, Goals and Understanding: An Inquiry into Human Knowledge Structures* p 191-199.

¹⁸⁹ Heron & Reason, 1997. *A Participatory Inquiry Paradigm* p 274.

sensory information connected through the organisational environment through which such interactions take place¹⁹⁰.

Interactions are further catalysed through a complex environment made up of processes, systems, routines, interpersonal, technical, and socio-cultural factors¹⁹¹. Knowledge in this environment is referred to as encultured knowledge, which is created through environment-based processes. In turn, this creates a shared socially based understanding in organisations¹⁹², constituted by an organisation's individuals. This relates to the cultural meaning of systems, which are also related to the processes of socialisation¹⁹³. These processes of socialisation are enacted through sets of individually based generalisations. The generalisations evolve collectively to create understanding through dialogue and rely on the organisational environment for the evolution of socially collaborative meaning¹⁹⁴.

Thirdly, regarding the knowledge transfer issue, knowledge is seen to flow from the intangible tacit dimension of the individual's internalised understanding¹⁹⁵ to either a tacit individual, tacit collective or explicit understanding. The issue of knowledge transfer in organisations is seen by some as predicated on the use and transfer of tacit knowledge to explicit knowledge, in response to the challenges posed by the business environment¹⁹⁶. From a collective view, this is brought about when individuals are grouped around particular contextual challenges or tasks¹⁹⁷. Individuals in this context enact sets of generalisations and historically evolved collective understandings¹⁹⁸ to produce new knowledge, which will likely be used in future interactions. From this point of view, tacit knowledge is contextualised with explicit knowledge and is situated around an individual's cognitive processes. Thus, tacit knowing creates explicit knowing and lends meaning to it, as a controlling factor for its uses¹⁹⁹. From an organisational

¹⁹⁰ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹⁹¹ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

¹⁹² Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹⁹³ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

¹⁹⁴ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 973.

¹⁹⁵ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹⁹⁶ Kwek, 1995. *Review: The Knowledge-Creating Company* p 2-3.

¹⁹⁷ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

¹⁹⁸ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 973.

¹⁹⁹ Polanyi, 1966. *The Logic of Tacit Inference* p 18.

perspective, this takes place through processes, networks, socialisation, development, interpretation, and the framing of knowledge²⁰⁰.

From an explicit view, the transfer of knowledge is seen to take place when individuals encode their knowledge as information and make it available to others²⁰¹. In this informational form, knowledge is thought of as readily transferable²⁰² and can be integrated into the processes of other individuals within the organisation. Further, knowledge transfer can take place through organisational learning processes. From this view an individual's embodied knowledge²⁰³ is shared as encultured knowledge in the form of collective understandings²⁰⁴, constituting an organisation's culture. Organisational culture is enacted through meaning and business processes, a part of which is organisational learning²⁰⁵. To create meaning, intangible knowledge assets are transferred from one entity to another through learning processes. This is done so individuals can visualise knowledge assets²⁰⁶ and their meaning within the confines of the organisation. It is also done so individuals can leverage the strategic value of these assets through the organisational environment, to create further meaning²⁰⁷ and thus competitive advantage. Encultured knowledge can then be codified as information, often in electronic forms²⁰⁸, resulting in the adoption of policy and procedures needed to govern organisational culture. Over time, these policies and procedures become explicitly engrained in the actions of individuals, forming part of the channels guiding the knowledge transfer process within organisations.

With these key issues of organisational knowledge in mind, Table 2-2 provides a matrix overlaying the three key knowledge issues of context/environment, social aspects, and knowledge transfer from an organisational perspective in the columns. The rows are made up of the various authors' definitions of knowledge. The intersection points of the matrix offer a *Yes* or *No* answer. The intersection points also highlight each definition's ability to meet the

²⁰⁰ Schank & Abelson, 1977. *Scripts, Plans, Goals and Understanding: An Inquiry into Human Knowledge Structures* p 191-199.

²⁰¹ Bellinger *et al.*, 2004. *Systems Thinking: Data, Information, Knowledge, and Wisdom*.

²⁰² Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

²⁰³ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

²⁰⁴ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

²⁰⁵ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1024.

²⁰⁶ Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 379.

²⁰⁷ Edvinsson & Kivikas, 2007. *Intellectual capital (IC) or Wissensbilans Process: Some German Experiences* p 379.

²⁰⁸ Blackler, 1995. *Knowledge, Knowledge Work and Organizations: An Overview and Interpretation* p 1025.

key issues of knowledge posed from an organisational perspective. The key issues have emerged from the tacit and explicit normalisation process. By intersecting the key organisational knowledge issues with the various definitions outlined in Table 2-1, definitions that are best placed to meet the requirements of an organisational definition of knowledge can be identified. Doing so will allow a compatible definition of organisational knowledge to be adopted going forward.

Table 2-2: Knowledge Definitions & Their Relationship to Key Organisational Knowledge Issues

Authors	Context/Environment	Social Aspects	Knowledge Transfer
Socrates (Plato, 1953)	No	No	No
Bacon (1605)	Yes	No	No
Boswell (1979)	Yes	No	Yes
Polanyi (1958, 1996)	Yes	No	Yes
Schank and Abelson (1977)	No	Yes	Yes
Frantzich (1983)	No	No	Yes
Anderson (1985)	Yes	No	No
Holliday and Chandler (1986)	No	No	No
Blackler. (1993)	Yes	Yes	Yes
Nonaka and Takeuchi (1995)	Yes	No	Yes
Heron (1996)	Yes	Yes	No
Tsoukas (1996)	Yes	Yes	Yes
Edvinsson and Malone (1997)	Yes	No	Yes

2.3 Adopting a Definition of Organisational Knowledge

Adopting a definition of knowledge that is well-aligned with the key organisational knowledge issues is important. It is important as it sets the foundation for an examination of how knowledge can be defined from an organisational perspective, as well as add context to the Becerra-Fernandez and Sabherwal framework. As can be seen from the Table 2-2, only two definitions of knowledge meet all the requirements of the key organisational knowledge issues. These are the definitions presented by Blackler and Tsoukas. While certain key issues are covered by other definitions of knowledge, the definitions of knowledge offered by Blackler

and Tsoukas are more complete and therefore relevant to defining knowledge from an organisational perspective without having to follow a piecemeal approach. As such, the other definitions that do not meet all the key knowledge issues are not as well-positioned to apply to the organisational context, when defining knowledge.

Tsoukas and Blackler follow a similar approach to defining organisational knowledge, in that they both take the view of the organisation as a distributed knowledge system. However, there are some key differences in their points of view. From Blackler's perspective, the focus in organisations should not be placed so much on knowledge, but rather on knowing. Regarding this point, Blackler outlines how organisational knowledge emphasis has moved away from embodied and embedded knowledge to embrained, encultured and encoded forms²⁰⁹ of knowledge. Blackler explains that focusing on knowing is important, as it overcomes many of the problems in the implication that knowledge relies on some universal truth²¹⁰. From this perspective, knowledge in organisations should be viewed as constituting part of an organisation's activity, a socially distributed element²¹¹, that forms part of the organisation's processes rather than remaining a separate entity. Organisational knowledge is not static, but rather something that is constantly evolving due to the contestations that exist in socially distributed systems. These contestations revolve around the organisational activities taking place between various problem solvers²¹². Blackler thus defines knowledge from an organisational point of view in several ways²¹³: 1) *Mediated* through systems and structures. 2) *Situated* in the context in which it happens. 3) *Provisional* due to knowledge's developing nature. 4) *Pragmatic* as knowledge is applied to tasks and activities. 5) *Contested* around the power situations between new problem solvers and their established counterparts.

Tsoukas and Vladimirou define organisational knowledge in two forms, taking a weak and a strong view²¹⁴. From the weak view, Tsoukas and Vladimirou define organisational knowledge simply as being generated, developed, and transmitted by individuals²¹⁵, which as they claim is less revealing about the deeper characteristics of what organisational knowledge is. From the

²⁰⁹ Blackler, 1995. *Knowledge, Knowledge Work and Organisations: An Overview and Interpretation* p 1038.

²¹⁰ Blackler, 1995. *Knowledge, Knowledge Work and Organisations: An Overview and Interpretation* p 1038

²¹¹ Blackler, 1995. *Knowledge, Knowledge Work and Organisations: An Overview and Interpretation* p 1038

²¹² Blackler, 1995. *Knowledge, Knowledge Work and Organisations: An Overview and Interpretation* p 1039

²¹³ Blackler, 1995. *Knowledge, Knowledge Work and Organisations: An Overview and Interpretation* p 1038-1042.

²¹⁴ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 979.

²¹⁵ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 979.

strong view, Tsoukas and Vladimirou claim that organisational knowledge emerges when individuals within organisations consider the context of their actions²¹⁶. They do so by drawing and acting upon a corpus of generalisations²¹⁷ which are produced internally because of organisational processes and tasks.

When comparing the definitions of both Tsoukas and Blackler, Tsoukas offers a definition of organisational knowledge that is theoretically deeper than that offered by Blackler. Blackler, on the other hand, aims to define organisational knowledge from a more practical perspective. It is an important distinction, as the aim of adopting a definition of knowledge is to frame what is meant by organisational knowledge from a KM and knowledge security perspective, as well as the key knowledge issues outlined in Table 2-2. Thus, it highlights the need to have a solid theoretical base of understanding to position knowledge security as a KM problem in organisations, from the perspective of the key knowledge issues.

This is not to say that Blackler's definition is not valuable for understanding knowledge in organisations. It offers value in that it is easily understood from a practical perspective. The crux of this, however, is that by being practically deeper it is also theoretically shallower than the definition offered by Tsoukas. There is also a point of contention that comes to light when examining Blackler's definition of organisational knowledge. This is the issue that Blackler raises concerning the contested nature of knowledge in organisations. Suggesting that knowledge needs to be contested from a base of power makes sense when looking at the flow and intersections of knowledge in an academic context, and rightly so.

However, from an organisational perspective, when it comes to contesting knowledge around tasks, the process runs the risk of causing social abrasion. Such abrasion could create an organisational environment where cohesion and the sharing of knowledge around tasks become less effective due to conflict. If this conflict were to manifest, it would have the opposite effect of applying and transferring knowledge around a task. Contesting knowledge runs the risk of people becoming more closed off to one another, decreasing knowledge sharing and generation. The tangible effect of this is that individuals will become less effective at completing tasks, which can result in lower levels of innovation taking place. If this is a persistent problem, it can in due course become a substantial risk for an organisation's competitiveness.

²¹⁶ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 979.

²¹⁷ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 979.

Tsoukas, by comparison, aims to avoid such issues by keeping his definition of organisational knowledge at a broader level. This allows Tsoukas to avoid the pitfalls of Blackler's definition relating to the contestation of knowledge; in terms of the knowledge processes taking place in the organisation. While I do agree that there is a need for some level of contestation to take place in organisations, as it creates new forms of knowing amongst participants, I disagree that such contestations need to be based on the power dynamics that Blackler suggests. Blackler's point implies an undue need for conflict in organisational knowing. This is not to say that such conflicts do not take place in real-world organisations, but the merits and productivity of leveraging such an approach must be questioned. Power-based conflict should not be established as the norm when defining knowledge processes but rather seen as an unwanted consequence that may occur from time to time through the process of socialisation.

These issues aside, the strength of both definitions lies in their ability to highlight the context and environment, social aspects, and knowledge transfer issues of organisational knowledge. This is particularly pertinent in that both definitions highlight the importance of viewing organisations as distributed knowledge systems. What sets apart Tsoukas' definition of knowledge is that he places a heavier emphasis on the tacit and explicit dimensions of knowledge in organisations. This means that Tsoukas' definition of organisational knowledge is more flexible in terms of analysing how knowledge works in organisations, not only in an explicit informational sense but also at a deeper tacit level. Therefore, making Tsoukas' definition of organisational knowledge more powerful and versatile.

As stated earlier, Tsoukas offers a strongly theoretical definition of organisational knowledge and due to this offers a deeper understanding of how knowledge processes function in organisations. By analysing organisational knowledge from Tsoukas' definition, it exposes many of the deeper issues which other definitions might not illuminate. Thus, using Tsoukas' definition of knowledge as a point of theoretical analysis, from a KM and knowledge security perspective, elevates this analysis beyond the bounds of traditional KM thinking. Tsoukas' definition is also more applicable in terms of advancing both KM and knowledge security theory than Blackler's definition. Tsoukas' definition allows a more in-depth understanding of organisational knowledge, where the focus of other definitions might only illuminate issues concerning knowledge systems, routines, and processes.

In addition, Tsoukas also offers a well-aligned definition regarding the key issues of organisational knowledge. From a context/environment perspective, Tsoukas places a heavy emphasis on the need for context and argues against the trend of other authors who attempt to

decontextualise knowledge. Through this de-contextualisation process, knowledge is viewed in the same light as the tangible resources of the organisation, meaning it is something that can be managed similarly. This is an incorrect assumption according to Tsoukas, as it can be intangible in nature.

Secondly, in terms of the social aspects issue, Tsoukas argues that knowledge cannot be created or shared without social interactions taking place. The intersection of business challenges with key individuals brings about this socialisation and the application, sharing, flow, and creation of knowledge around organisational tasks. In this regard, Tsoukas avoids Blackler's approach by not positioning his definition of knowledge as dependent upon power-based contestations. Yet, Tsoukas does not forget to highlight the importance of social interactions as part of the organisational knowledge processes.

Thirdly, in terms of the knowledge transfer issue, Tsoukas argues that knowledge cannot be transferred as an entity or product as some authors would like. Instead, knowledge is derived from socialisation and internalised or shared through the process of applying an individual's knowledge to a particular context. This knowledge can then be refined according to what is being shared with the individual, based on other individuals' actions around organisational tasks. Through these actions, the individual will integrate those cues and meanings with that of their own. This is done not by transferring knowledge as a tangible entity, but rather by incorporating knowledge within an individual's perceptions and ideologies to make their own meaning.

Knowledge from Tsoukas' perspective is not something that can be copied from one individual and simply uploaded to another. Rather, it relies on context, where the perceptions and socialisation between individuals must be present to offer any real value in the transfer of tacit knowledge. It can also be presumed that explicit knowledge, unlike tacit knowledge, due to its explicit form, is easily transferred. However, this is not entirely the case. The transfer of explicit knowledge is routed in the tacit, as it relies upon an individual's interaction with information. This interaction in each context is filtered through an individual's generalisations, framed by their knowledge, to interpret and add meaning to the explicit form of knowledge they are dealing with. Therefore, this process cannot be successful without tacit knowledge, as an individual's tacit knowledge will govern how they interpret explicit knowledge and what meaning it holds for them based on their perceptions and internalised beliefs.

Considering Tsoukas' view of tacit and explicit knowledge, of a particular contest for Tsoukas is the view of tacit and explicit knowledge argued by Nonaka and Takeuchi in their major work *The Knowledge Creating Company*, which has been widely adopted in management studies. Tsoukas disagrees with Nonaka and Takeuchi's view that tacit knowledge is a definable thing in organisations that can be captured and transferred from one person to another. This is because Tsoukas holds special relevance for the human emphasis in defining knowledge, as given in the work of Polanyi, regarding Polanyi's views of tacit and explicit knowledge. Tsoukas builds upon Polanyi's view of tacit and explicit knowledge, by outlining that a realignment of the current definitions of organisational knowledge is needed; to move them closer to the original ideas expressed by Polanyi²¹⁸. According to Tsoukas, this is because the generation, application and contextualisation of knowledge are currently misunderstood²¹⁹. Tsoukas' conflicting view, with the argument set out by Nonaka and Takeuchi, is outlined by Tsoukas in the following extract.

Tacit knowledge has been greatly misunderstood in management studies... Nonaka and Takeuchi's interpretation of tacit knowledge as knowledge not yet articulated – knowledge waiting for its 'translation' or 'conversion' into explicit knowledge – an interpretation that has been widely adopted in management studies, is erroneous: it ignores the essential ineffability of tacit knowledge, thus reducing it to what can be articulated. Tacit and explicit knowledge are not the two ends of a continuum but the two sides of the same coin: even the most explicit kind of knowledge is underlain by tacit knowledge. Tacit knowledge consists of a set of particulars of which we are subsidiarily aware as we focus on something else. Tacit knowledge is vectorial: we know the particulars by relying on our awareness of them for attending to something else. Since subsidiaries exist as such by bearing on the focus to which we are attending from them, they cannot be separated from the focus and examined independently, for if this is done, their meaning will be lost... The ineffability of tacit knowledge does not mean that we cannot discuss the skilled performances in which we are involved. We can – indeed, should – discuss them provided we stop insisting on 'converting' tacit knowledge and, instead, start recursively drawing our attention to how we draw each other's attention to things. Instructive forms of talk help us re-orientate ourselves to how we relate to others and the world around us, thus enabling us to talk and act differently. We can command a clear view of our

²¹⁸ Tsoukas, 2002. *Do we Really Understand Tacit Knowledge?* p 4-10.

²¹⁹ Tsoukas, 2002. *Do we Really Understand Tacit Knowledge?* p 4-10.

tasks at hand if we ‘remind’ ourselves of how we do things so that distinctions which we had previously not noticed, and features which had previously escaped our attention, may be brought forward²²⁰.

With these points in mind, I will provide an overview of Tsoukas’ view of organisational knowledge. This must be done to expand upon Tsoukas’ definition of organisational knowledge by providing the relevant background for it, based on Tsoukas’ view of organisations as distributed knowledge systems. I will discuss this by considering the roles of tacit and explicit knowledge and their function in organisations, as assigned by Tsoukas. Doing so will set the stage for a brief analysis of the benefits and detriments of making use of Tsoukas’ definition of organisational knowledge. I will also explore its applicability for adding context to the Becerra-Fernandez and Sabherwal framework, as well as helping to better understand KM and knowledge security practices in organisations. All of which will be useful for conceptualising the relationship between knowledge security and KM.

2.3.1 Overview of Tsoukas’ Definition of Organisational Knowledge

Tsoukas’ definition of organisational knowledge aims to clarify the relationship between tacit and explicit knowledge in organisations²²¹. He does this by emphasising the role that tacit knowledge plays in organisations, stating that explicit knowledge cannot exist without tacit knowledge²²². This he frames as a knowledge transfer issue, in terms of the capability of the members of an organisation to draw distinctions in the process of carrying out their work, rather than looking to define the actual transfer of tacit knowledge to explicit knowledge, which Tsoukas explains is an erroneous view²²³. How Tsoukas views knowledge, and the transfer of knowledge in organisations, is predominantly centred on the socialisation processes that take place to meet organisational tasks. This is expressed in the following extract by Tsoukas and Vladimirou as per their definition of knowledge.

Organisational knowledge is the capability members of an organisation have developed to draw distinctions in the process of carrying out their work, in particular

²²⁰ Tsoukas, 2002. *Do we Really Understand Tacit Knowledge?* p 4-10.

²²¹ Kakabadse *et al.*, 2003. *Reviewing the Knowledge Management Literature: Towards a Taxonomy* p 79.

²²² Crane, 2013. *A New Taxonomy of Knowledge Management Theory: The Turn to Knowledge as Constituted in Social Action* p 1-20.

²²³ Tsoukas, 2002. *Do we Really Understand Tacit Knowledge?* p 1.

concrete contexts, by enacting sets of generalisations whose application depends on historically evolved collective understandings²²⁴.

As is clear from this definition, Tsoukas emphasises the collective understandings of individuals within an organisation in terms of knowledge generation and meaning. Tsoukas and Vladimirou explain that one should not take a narrow view of knowledge in organisations as purely cognitive but focus more on the process and socialisation elements²²⁵. Tsoukas and Vladimirou warn that there are several unanswered questions relating to what merits organisational knowledge and how knowledge can become an individual possession²²⁶. They state that this is best overcome by offering not only a theory of knowledge but also a theory of organisation.

Realising that knowledge is indeed a tricky concept, some researchers have gone as far as to suggest (mostly in the context of academic conferences) that, perhaps, we do not need more formal definitions of knowledge, since they, very likely, end up complicating things further. We do not agree with this view. Our understanding of organisational knowledge (or any other topic of interest) will not advance if we resign ourselves to merely recycling commonsensical notions of knowledge for, if we were to do so, we would risk being prisoners of our own unchallenged assumptions, incapable of advancing our learning. On the contrary, what we need is ever more sophisticated theoretical explorations of our topic of interest, aiming at gaining a deeper insight into it²²⁷.

Considering this view, the key perspective is how Tsoukas views organisations as distributed knowledge systems. These distributed systems, Tsoukas argues, are governed by six key facets: 1) The resources of an organisation are not given or discovered but created. 2) The organisational problem firms face in the utilisation of knowledge cannot be known in its totality by a single mind. 3) The firm is a distributed knowledge system. 4) A firm's knowledge is distributed in an additional sense; it is partly derived from the broader industrial and societal context within which a firm is embedded. 5) Normative expectations, dispositions, and interactive situations are inevitably in tension. 6) Viewing a firm as a distributed knowledge

²²⁴ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 973.

²²⁵ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 974.

²²⁶ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 974.

²²⁷ Tsoukas & Vladimirou, 2001. *What is Organisational Knowledge?* p 974.

system helps to refine the view of what organisations are, and consequently of what KM processes are about²²⁸. I will briefly outline these key facets in the paragraphs to follow.

Expanding upon the first of these six facets, Tsoukas argues that “it is not so much the resources *per se* that are important to a firm as the services rendered by those resources (Penrose, 1959)”²²⁹. Tsoukas outlines that the services rendered depend on how those resources are viewed by members of the organisation in each context²³⁰. What Tsoukas means by this is that the use of resources in an organisation can be considered a function of the knowledge which is applied to them. The way knowledge is applied to the resources is carried out through an organisation’s routines²³¹. When these resources are combined with the social processes involved with member interactions, innovation emerges. Tsoukas states that “the carriers of such knowledge are a firm’s routines (Nelson and Winter, 1982) and, from the point of view of how novelty emerges, a firm’s members”²³². Adopting this view, an organisation is a system through which knowledge is carried, via its routines, and dynamically applied to a given context by its members in dealing with a specific task. An organisation can thus be viewed as an entity through which knowledge flows systematically.

Tsoukas’ second facet is that “the organisation problem firms’ face is the utilisation of knowledge, which is not, and cannot be, known in its totality by a single mind”²³³. Knowledge is not the realm of a single individual but rather the use and product of the collective. Building on this view, Tsoukas’ third facet argues that “the firm is a *distributed* knowledge system”²³⁴, and as such it requires the coming together of disparate entities to apply and create new knowledge²³⁵ around organisational tasks. Organisational knowledge is not only distributed in the computational sense or the sense that the factual knowledge of the circumstances of time and place cannot be surveyed as a whole²³⁶. An organisation’s knowledge, according to Tsoukas, is distributed in the sense that it is inherently indeterminate. Tsoukas states that “nobody knows in advance what that knowledge is, or need be. Firms are faced with *radical*

²²⁸ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 21-22.

²²⁹ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 21.

²³⁰ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 21.

²³¹ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 21.

²³² Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 21.

²³³ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 21.

²³⁴ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²³⁵ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²³⁶ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

uncertainty: they do not, they cannot, know what they need to know”²³⁷. Tsoukas goes on to explain that organisations are not only distributed systems, but they are also decentred systems²³⁸. What he means by this is that they lack a centralised cognitive equivalent of a “control room”²³⁹ as knowledge application, creation and use come together in an ad hoc manner.

The fourth facet that Tsoukas outlines is that “a firm’s knowledge is distributed in an additional sense, namely that it is partly derived from the broader industrial and societal context within which a firm is embedded (Granovetter, 1992; Spender, 1989; Whitley, 1996)”²⁴⁰. Tsoukas states that “a firm’s knowledge is continually (re)constituted through the activities undertaken within a firm. The latter’s knowledge is not, and cannot be, self-contained”²⁴¹. Organisational knowledge not only exists internally, within the realm of its individuals, but is also impacted by how those individuals’ perceptions have been moulded from the external environment in which they operate. Tsoukas outlines in the fifth facet of his argument that normative (established) expectations, dispositions (character), and interactive situations are always in tension²⁴². This point is explained further in conjunction with the other facets discussed above in the following extract by Tsoukas.

A firm has (greater or lesser) control over normative expectations, whereby the behaviour of its members is sought to be made consistent across contexts. However, a firm has no control over its members’ dispositions, which are derived from their past socialisations in contexts outside the firm. Finally, the normative expectations and dispositions of the members of a firm are instantiated within particular interactive situations, whose features cannot be fully known by anyone *ex ante* but are actively shaped by practitioners as they confront local circumstance. Thus, a firm’s knowledge is emergent (Weick and Roberts, 1993): it is not possessed by a single agent; it partly originates ‘outside’ the firm; and it is never complete at any point”²⁴³.

²³⁷ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²³⁸ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²³⁹ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴⁰ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴¹ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴² Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴³ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

Tsoukas advises that there are always gaps that will exist between these different dimensions in addition to normative expectations, dispositions, and interactive situations. These tensions exist between various areas²⁴⁴: 1) Official organisational practice and non-official organisational practice. 2) Universal and exclusive practices. 3) Formal and corroborative rationality. 4) Ideal and practical action. 5) Rules as presented and rules as guides in practice. 6) The model of reality and the reality of the model. Tsoukas contends that these gaps can only be closed through practitioners exercising their judgement. This judgment is based on the features that practitioners have decided are relevant, for each one of the three dimensions, making up the social practices that contribute towards innovation, normative expectations, dispositions, and interactive situations.

From the preceding analysis, it follows that how normative expectations, dispositions and interactive situations are matched is always a contingent, emergent, indeterminate event. From a research point of view, what needs to be explained is not so much ‘why firms differ’... as what are the processes that make them similar – how the infinitude of particularities is tamed, how tensions are managed, and gaps are filled; how, in short, in a distributed knowledge system coherent action emerges over time”²⁴⁵.

Tsoukas’ sixth facet concerns the management implications of viewing the organisation as a distributed knowledge system²⁴⁶. According to Tsoukas, examining these implications allows us to “refine our view of what organisations are and, consequently, of what management is about”²⁴⁷. From the facets covered, organisations are not static entities, thus knowledge generation and innovation are carried forward and “novel practices are never exhausted”²⁴⁸. Based on this view, in terms of managing knowledge in organisations, the practice can then be viewed as coordinating the right individuals based upon the requirements of the task, and how those individuals interpret context. Sharing expertise and knowledge is coordinated through the mechanism of the organisation. This view is explained by Tsoukas in the following extract.

Organisational members do follow rules but how they do so is an inescapably contingent-cum-local matter. In organisations, both rule-bound action and novelty are present, as are continuity and change, regularity and creativity. Management,

²⁴⁴ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴⁵ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴⁶ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴⁷ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

²⁴⁸ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 22.

therefore, can be seen as an open-ended process of coordinating purposeful individuals, whose actions stem from applying their unique interpretations to the local circumstances confronting them. Those actions give rise to often unintended and ambiguous circumstances, the meaning of which is open to further interpretations and further action, and so on. Given the distributed character of organisational knowledge, the key to achieving coordinated action does not so much depend on those ‘higher up’ collecting more and more knowledge, as on those ‘lower down’ finding more and more ways of getting connected and interrelating the knowledge each one has. A necessary condition for this to happen is to appreciate the character of the firm as a discursive practice: a form of life, a community, in which individuals come to share an unarticulated background of common understandings. Sustaining a discursive practice is just as important as finding ways of integrating distributed knowledge”²⁴⁹.

2.3.2 The Risks and Benefits of Using Tsoukas’ Definition of Organisational Knowledge

Although Tsoukas’ definition highlights many of the important theoretical elements when it comes to organisational knowledge, it is not free from risk. Firstly, Tsoukas’ definition of knowledge is largely based on theory. While this is a benefit of Tsoukas’ approach, there is also a level of risk involved, in that some of the practical elements of the knowledge processes in organisations could be overlooked. As such, one could argue that a definition akin to that offered by Blackler would be better suited for categorising organisational knowledge from a practical perspective. Blackler’s definition could contextualise organisational knowledge, KM, and knowledge security practices more tangibly. I would argue, however, that the level of risk posed by potential practical oversight is low. To mitigate this risk, it is pertinent to conduct a more careful analysis of the selection of aspects in KM that are being examined, considering the need to have a theoretically deeper definition of organisational knowledge. The benefits of doing so will far outweigh the risks posed, as definitive practical alignment is not what is being examined here and will in any case be provided in part by the Becerra-Fernandez and Sabherwal KM framework.

Secondly, it could also be argued that the broadness of Tsoukas’ definition can be a hindrance to understanding knowledge in organisations. From this perspective, Tsoukas’ definition of organisational knowledge could struggle to convey meaning if it is lacking context. As such, it

²⁴⁹ Tsoukas, 1996. *The Firm as a Distributed Knowledge System: A Constructionist Approach* p 23.

could also be argued that more practical or individualistic definitions of organisational knowledge can overcome this pitfall, by not placing a heavy emphasis on context to determine what organisational knowledge is. However, to argue that Tsoukas' definition of organisational knowledge could be understood without context is to miss much of the meaning of the definition. From a practical perspective, Tsoukas' definition becomes powerful as soon as context is added. Since Tsoukas continually re-emphasises the importance of the human element in understanding organisational knowledge, it is counterintuitive to try to analyse organisational knowledge without context. Individuals always rely on some form of context, whether internal or external, to guide their application, integration, and generation of knowledge in organisations. Organisations, and by extension individuals, are not free from context when dealing with organisational knowledge.

Thirdly, unlike authors such as Nonaka and Takeuchi, who provide a populist view of organisational knowledge, due to the theoretical nature of Tsoukas' definition, it is arguably too complicated. It runs the risk of being too theoretical and convoluted for managers working in organisations to grasp easily, as it is a very philosophical approach. This can be a risk; in that it creates an undue hindrance to the application of Tsoukas' definition in practice. However, from a research perspective, given the need to contextualise Becerra-Fernandez and Sabherwal's KM framework and knowledge security, it is more beneficial. It allows for a much deeper analysis of what organisational knowledge is. Given that for this dissertation a strong theoretical definition is needed, Tsoukas' definition is well suited for this task, thus reducing risk in this instance.

With these risks in mind, there are also several benefits to using Tsoukas' definition of organisational knowledge. Firstly, Tsoukas moves beyond a simplified definition of what organisational knowledge is, as often seen in individualistic or entity-based approaches²⁵⁰. The strength of Tsoukas' approach is that it facilitates an understanding of knowledge across the length and breadth of the organisation, as well as its impacts as a distributed entity. Secondly, by following the distributed view offered by Tsoukas, it enables a position on organisational knowledge that is free from the limitations of other views. An attempt is made to categorise different types of knowledge for contexts, situations, processes, interactions, or facilitations. Thus, Tsoukas' view is not hindered by the contextual limitations of these definitions, and as such is more universally applicable, when trying to understand knowledge from an

²⁵⁰ Felin & Hesterly, 2007. *The Knowledge-Based View, Nested Heterogeneity, and New Value Creation: Philosophical Considerations of the Locus of Knowledge* p 195-196.

organisational perspective. Thirdly, as Tsoukas offers a tacit and explicit based distributed view of organisational knowledge, his definition ties in well with the broader views of how knowledge should be managed in the structural sense within organisations. By doing so, Tsoukas can offer context to organisational meaning, in so much as it allows for an understanding of the role of knowledge, socialisation and interaction at various intersections within the organisation, as part of its KM processes.

2.4 Conclusion

Chapter 2 formed the first part of the theoretical analysis and aimed at outlining the existing definitions of the concept of organisational knowledge using a literature review. This is in line with the research question focused on examining how knowledge is thought about and defined from an organisational perspective, as illustrated in Figure 1-2²⁵¹. To achieve this aim, the discussion was contextualised through the organisational management parent body of literature. The key definitions of knowledge through the ages were presented and then normalised using a tacit and explicit point of view as a common leveller. Following this discussion, a definition of organisational knowledge was adopted and discussed. Doing so acts as a precursory measure to overcome the agnostic limitations of Becerra-Fernandez and Sabherwal's KM framework, as discussed in Chapter 1. With this understanding in mind, in Chapter 3, I will proceed to outline and examine the key positions as they relate to KM. I will investigate how these positions enable an integrated need for knowledge security, as an opportunity to contextualise Becerra-Fernandez and Sabherwal's KM framework. This will form the second part of the theoretical analysis and pertains to the research objectives of examining the key theoretical issues and positions in the literature as they relate to KM, how KM can be defined and why there is a need to integrate knowledge security and KM.

²⁵¹ Research sub-question 2.1: *How can knowledge be thought about and defined from an organisational perspective?*

Chapter 3

Defining Knowledge Management

3.1 Introduction

The chapter consists of a review of the key issues and positions in the literature as they relate to KM. This is analysed from the sense of how such issues and positions enable an integrated need for knowledge security. Thus, I begin by firstly examining why KM is important for today's organisations to establish context. Building on this context, I then outline the key theoretical issues and positions in KM. With this context in mind, I then discuss the problems that arise when defining KM and aim to overcome them by arguing for a consolidated definition.

3.2 The Rise in Importance of Knowledge Management

Webster²⁵² argues that it is accepted that information and knowledge have achieved a special place in the contemporary world, what some call the information or knowledge society²⁵³. This is particularly true of the business environment in which today's organisations operate, where information and knowledge have become a key business resource for generating innovation and competitive advantage²⁵⁴. The special importance of information and knowledge contrasts with industrial age thinking, where work and the management of organisations were thought of and managed from a mechanistic perspective.

As an academic discipline, management is much younger. Frederick Winslow Taylor is often cited as the founder of management studies. His 1911 book "The Principles of Scientific Management" portrays managers as organizers: they arranged cogs in the industrial machine. Their job was about increasing efficiency and productivity. For Taylor, management "studies" meant standing in a workplace

²⁵² Webster, 2006. *Theories of the Information Society* p 6.

²⁵³ Webster, 2006. *Theories of the Information Society* p 6.

²⁵⁴ Cabrera-Suárez *et al.*, 2001. *The Succession Process from a Resource and Knowledge-Based View of the Family Firm* p 38.

with a stopwatch, measuring workers' actions, and devising ways to eliminate "all false movements, slow movements and useless movements"²⁵⁵.

Drucker was the first to highlight the difference between Taylor's industrial thinking and post-industrial thinking, concerning the nature of work²⁵⁶, by coining the term "knowledge worker"²⁵⁷. Drucker saw this shift to knowledge work as the evolution of industrial thinking²⁵⁸. Murray²⁵⁹ explains that by this term Drucker was referring to people whose work primarily involves the manipulation of information and knowledge rather than manual labour as the means of production.

The knowledge worker's contribution to an enterprise couldn't be measured with a stopwatch or a punch card. It couldn't be forced or controlled by any amount of oversight. And it couldn't be encouraged by simple pay schemes tied to hourly output²⁶⁰.

The view of employees functioning in an information or knowledge dependent world, rather than a mechanistic paradigm, is not without controversy. Webster points out²⁶¹ that there are those in the literature who debate the credibility of the concept of the information or knowledge society as something radically new or rather as a continuum of the industrial revolution. However, as Webster also argues²⁶², there is no discord as to the importance of information and knowledge in our society, the key factor at hand in this context. Thus, whatever view one may hold, it remains important for organisations to be able to glean business value from their knowledge. Knowledge must be leveraged in the business environment by an organisation's workers in such a way to create innovation²⁶³ and thereby increase competitive advantage for the organisation.

In the past few years, however, there has been a raging interest in treating knowledge as a significant organisational resource. The heightened interest in organisational knowledge and knowledge management stems from the transition into the

²⁵⁵ Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁵⁶ Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁵⁷ Drucker cited in Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁵⁸ Drucker cited in Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁵⁹ Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁶⁰ Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁶¹ Webster, 2006. *Theories of the Information Society* p 2.

²⁶² Webster, 2006. *Theories of the Information Society* p 2.

²⁶³ Liu, S. 2002. *University of North Carolina - Introduction to Knowledge Management* [Online].

knowledge economy, where knowledge is viewed as the principal source of value creation and sustainable competitive advantage²⁶⁴.

Organisational innovation, which leads to competitive advantage, is manifested through the use, application, and integration of KM practices within organisational processes, whether these knowledge-based activities are called KM or not²⁶⁵. This is done to benefit the organisation by increasing its competitive advantage in the market²⁶⁶. Du Plessis²⁶⁷ identifies three main drivers related to the process involved in applying KM to organisations as a tool for innovation and competitiveness.

According to the literature there are three main drivers of the application of knowledge management in innovation. The first basic driver for knowledge management's role in innovation in today's business environment is to create, build and maintain competitive advantage through utilization of knowledge and through collaboration practices... The second driver of the role of knowledge management in innovation is that knowledge is a resource used to reduce complexity in the innovation process, and managing knowledge as a resource will consequently be of significant importance... The third driver of applying knowledge management to the benefit of the innovation process is the integration of knowledge both internal and external to the organisation, thus making it more available and accessible²⁶⁸.

Therefore, unlike the industrial based period of economic activity, an organisation operating in a knowledge-based economy cannot reach a high level of success without the use, application, and management of its knowledge resources²⁶⁹. As such, a prominent facet in the evolution of KM was the merging of various management disciplines. Chang-Albitres and Kruger²⁷⁰ explain that what is seen as KM today is a result of research started in the 1970s at the Massachusetts Institute of Technology and Carnegie Mellon. The research emerged out of the consolidation of diverse disciplines including organisational science, human resources (HR) management,

²⁶⁴ Alavi & Leidner, 2001. *Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues* p 1-79.

²⁶⁵ Giedts, 2013. *Looking for a New Name for Knowledge Management* [Online].

²⁶⁶ Ndlela & du Toit, 2001. *Establishing a Knowledge Management Programme for Competitive Advantage in an Enterprise* p 160.

²⁶⁷ du Plessis, 2007. *The role of knowledge management in innovation* p 22-23.

²⁶⁸ du Plessis, 2007. *The role of knowledge management in innovation* p 22-23.

²⁶⁹ Shear, 2009. *Business Counterintelligence: Sustainable Practice or Passing Fad?* p 13-30.

²⁷⁰ Chang-Albitres & Krugler, 2005. *A Summary of Knowledge Management Information Gathered from Literature, Websites and State Departments of Transportation* p 3.

computer science, management information systems, management science, psychology, and sociology²⁷¹.

It was the Carnegie school, best exemplified by the work of Richard M. Cyert and James G. March (Cyert and March 1963), that transformed these rudimentary and largely anecdotal observations into a formal theory of organizational learning and KM... Four decades later, the field is characterized by a wealth of empirical evidence and a wide array of theoretical perspectives... The highly differentiated nature of organizational learning and KM is the hallmark of the field and is evident in the multitude of disciplinary perspectives brought to bear on the topic²⁷².

Due to this shift in industrial era mechanistic thinking²⁷³, KM emerged as a tool to deal with the challenges posed by the knowledge-based business environment. Murray²⁷⁴ outlines that Drucker suggests deconstructing today's managers' jobs into five key objectives: 1) To set defined objectives. 2) Delegate work into achievable chunks. 3) Motivate and communicate with employees. 4) Measure performance. 5) Develop people through training²⁷⁵. Serban and Luan²⁷⁶ point out that in the early 1990s corporations began to formally coin the term KM, under the guise of a systematic effort to capitalise on the cumulative knowledge at their disposal. Additional reasons for adopting KM practices also included: trying to deal with information overload and chaos, information congestion, skill segmentations and specialisation, workforce mobility, employee turnover, and competition within the business environment²⁷⁷.

This diverse legacy has resulted in a broad array of approaches to KM being developed without one unique, universally accepted method of implementing KM across the board²⁷⁸. The development of KM has also been aligned with how organisations viewed knowledge in these

²⁷¹ Chang-Albitres & Krugler, 2005. *A Summary of Knowledge Management Information Gathered from Literature, Websites and State Departments of Transportation* p 3.

²⁷² Argote *et al.*, 2003. *Managing Knowledge in Organisations: An Integrative Framework and Review of Emerging Themes* p 571.

²⁷³ Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁷⁴ Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁷⁵ Murray, 2010. *As Work Changes So Must Managers* [Online].

²⁷⁶ Serban & Luan, 2002 *Overview of Knowledge Management* p 5.

²⁷⁷ Serban & Luan, 2002 *Overview of Knowledge Management* p 6-7.

²⁷⁸ Chang-Albitres & Krugler, 2005. *A summary of Knowledge Management Information Gathered from Literature, Websites and State Departments of Transportation* p 3.

contexts, either as being tacit or explicit²⁷⁹, and the relationship between the two terms. It has also played a role in the implementation of KM in organisations, the kinds of KM processes and tools that they have adopted²⁸⁰, and the different theoretical KM positions taken in the literature.

3.3 Key Theoretical Positions in Knowledge Management

The term KM was first used in its current form as early as 1987 for an internal study on information handling and utilisation at McKinsey²⁸¹. Historically as Koenig states, “KM went public, as it were, at a conference in Boston in 1993 organised by Ernst and Young”²⁸². From there, one of the first definitions of KM was offered by Davenport, who was at Ernst and Young at the time²⁸³. Davenport states that “KM is the process of capturing, distributing and effectively using knowledge”²⁸⁴. Koenig²⁸⁵ contends that in their opinion this is still to date one of the better single-line definitions of KM that has appeared in the literature.

In his later work, Davenport built on this perspective further by stating that organisations should aim to focus on the lateralised flow of information. To support this focus, tools and techniques are implemented²⁸⁶ to increase the effectiveness of the lateralised flow. An example of this is the use and application of social software platforms and technologies²⁸⁷ for increasing the creation and sharing of organisational knowledge. Davenport’s approach also focused on the perspective that organisations manage their knowledge around centralised repositories. This approach aims to concentrate management initiatives on transferring tacit knowledge into an explicit form which is then stored in centralised knowledge repositories.

Another position on KM is that of the value-driven approach offered by Wiig²⁸⁸, which is based on two key objectives²⁸⁹. The first is to make sure that the enterprise acts as intelligently as

²⁷⁹ Chang-Albitres & Krugler, 2005. *A summary of Knowledge Management Information Gathered from Literature, Websites and State Departments of Transportation* p 6.

²⁸⁰ Curado *et al.*, 2011. *Mapping Knowledge Management Authoring Patterns and Practices* p 5.

²⁸¹ Koenig, 2018. *What is KM? Knowledge Management Explained* [Online].

²⁸² Koenig, 2018. *What is KM? Knowledge Management Explained* [Online].

²⁸³ Koenig, 2018. *What is KM? Knowledge Management Explained* [Online].

²⁸⁴ Davenport, 1994. *Saving ITs Soul: Human Centred Information Management* p 119-131.

²⁸⁵ Koenig, 2018. *What is KM? Knowledge Management Explained* [Online].

²⁸⁶ Davenport, 2008. *Enterprise 2.0: The New, New Knowledge Management* [Online].

²⁸⁷ McAfee, 2006. *Enterprise 2.0 Inclusionists and Deletionists* [Online].

²⁸⁸ Wiig, 1997. *Knowledge Management: Where Did It Come from and Where Will It Go?* p 1.

²⁸⁹ Wiig, 1997. *Knowledge Management: Where Did It Come from and Where Will It Go?* p 1.

possible to secure its viability and overall success²⁹⁰. The second is to realise the value of the organisation's knowledge assets²⁹¹. Wiig states that this is achieved through several processes, namely: "top-down monitoring and facilitation of knowledge activities; creation and maintenance of knowledge infrastructure; renewing, organising, and transferring knowledge assets; and using knowledge assets to realise their value"²⁹².

Conner and Prahalad²⁹³ offer a different position on KM, recommending that organisations take a social and hierarchical approach. They suggest that the way individuals in an organisation cooperate will affect and influence the knowledge that they apply to business activity framed by the organisation²⁹⁴. This perspective is what Conner and Prahalad call the "resource-based theory of the firm"²⁹⁵. Depending on the situation, different knowledge can be brought to bear which will affect the outcome of the completion of the task based on the collective interaction of individuals associated with that task²⁹⁶.

In outlining KM, Drucker²⁹⁷ takes a management theorist position to KM. Drucker's position suggests that knowledge work in organisations should revolve around five key factors²⁹⁸. Summarised, these factors are: correctly identifying tasks; self-management of activity; increasing innovation; continuous learning and teaching; and quality of output, where intellectual capital is recognised and valued²⁹⁹. All such work should be aligned with the systems in place in the organisation³⁰⁰ and feed the organisation's innovation, decision and learning processes.

Senge builds on this position by arguing that organisations have moved from a resource-based view of the firm to a knowledge-based perspective³⁰¹. Central to this position are the concepts

²⁹⁰ Wiig, 1997. *Knowledge Management: Where Did It Come from and Where Will It Go?* p 1.

²⁹¹ Wiig, 1997. *Knowledge Management: Where Did It Come from and Where Will It Go?* p 1.

²⁹² Wiig, 1997. *Knowledge Management: Where Did It Come from and Where Will It Go?* p 2.

²⁹³ Conner & Prahalad, 1996. *A Resource-Based Theory of the Firm: Knowledge Versus Opportunism* p 477.

²⁹⁴ Conner & Prahalad, 1996. *A Resource-Based Theory of the Firm: Knowledge Versus Opportunism* p 477.

²⁹⁵ Conner & Prahalad, 1996. *A Resource-Based Theory of the Firm: Knowledge Versus Opportunism* p 477.

²⁹⁶ Conner & Prahalad, 1996. *A Resource-Based Theory of the Firm: Knowledge Versus Opportunism* p 477.

²⁹⁷ Drucker, 1999. *Knowledge-Worker Productivity: The Biggest Challenge* p 83-84.

²⁹⁸ Drucker, 1999. *Knowledge-Worker Productivity: The Biggest Challenge* p 83-84.

²⁹⁹ Drucker, 1999. *Knowledge-Worker Productivity: The Biggest Challenge* p 91.

³⁰⁰ Drucker, 1999. *Knowledge-Worker Productivity: The Biggest Challenge* p 91.

³⁰¹ Senge, 1991. *Transforming the Practice of Management* p 87.

of learning and a shared vision to enable good decisions and inspire people³⁰². Senge³⁰³ argues that it is critical to hold a shared vision of accomplishment in line with learning practices. Otherwise, the focus and energy for learning will seem abstract and meaningless.

Klein's³⁰⁴ position on KM is framed from a strategy and competitiveness standpoint. Klein outlines that organisations need to manage and leverage their intellectual capital in a systematic way, in the face of a cutthroat world of competitiveness³⁰⁵. If an organisation is to survive, it must be able to manage its competitive advantage systematically and share ideas across functional boundaries. Klein suggests that organisations need to devise strategies, portfolios, and initiatives to capture and share ideas if they are to remain competitive³⁰⁶.

In an environment where innovations are replicated by competitors expeditiously and where smaller firms often gain market share from larger ones by introducing superior products and services, it is firms' intellectual capital – their knowledge, experience, expertise, and associated soft assets, rather than their hard physical and financial capital – that increasingly determines their competitive positions... In particular organizations are devising enterprise strategies and portfolios of initiatives to capture and disseminate what they learn over time, to facilitate the sharing of new ideas and experiences across functional and organizational boundaries, to leverage their best practices, and to manage their intellectual capital by other deliberate means rather than continuing to rely on haphazard approaches³⁰⁷.

Becerra-Fernandez and Sabherwal view KM as “simply doing what is needed to get the most out of knowledge resources”³⁰⁸. As they outline, this means that the traditional emphasis of KM has been on “knowledge that is recognised and already articulated in some form”³⁰⁹. In practice, this includes knowledge about processes, procedures, IP, best practices, forecasts, lessons learned, and solutions to problems that keep recurring³¹⁰. They explain that KM has also focused on managing the knowledge that exists in the minds of an organisation's

³⁰² Senge, 1991. *Transforming the Practice of Management* p 87.

³⁰³ Senge, 1990. *The Fifth Discipline: The Art and Practice of the Learning Organisation* p 206.

³⁰⁴ Klein, 2009. *The Strategic Management of Intellectual Capital: An Introduction* p 1.

³⁰⁵ Klein, 2009. *The Strategic Management of Intellectual Capital: An Introduction* p 1.

³⁰⁶ Klein, 2009. *The Strategic Management of Intellectual Capital: An Introduction* p 1.

³⁰⁷ Klein, 2009. *The Strategic Management of Intellectual Capital: An Introduction* p 1.

³⁰⁸ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

³⁰⁹ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

³¹⁰ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

experts³¹¹. From this perspective, they position KM as more of an enabling factor for managing different types of intellectual capital³¹².

An organization's intellectual capital refers to the sum of all its knowledge resources, which exist in aspects within or outside the organization (Nahapiet and Ghoshal 1998). There are three types of intellectual capital: human capital, or the knowledge, skills, and capabilities possessed by individual employees; organizational capital, or the institutionalized knowledge and codified experience residing in databases, manuals, culture, systems, structures, and processes; and social capital, or the knowledge embedded in relationships and interactions among individuals (Subramaniam and Youndt 2005)³¹³.

From this perspective, KM is seen as an increasingly important entity that helps to promote the creation, sharing and leveraging of an organisation's knowledge³¹⁴. In other words, the primary mechanism used to manage an organisations knowledge resource³¹⁵. This means focusing, organising, and making available important knowledge, wherever and whenever it is needed³¹⁶. Becerra-Fernandez & Sabherwal state that the benefits of doing so include: "leveraging core business competencies, accelerating innovation and time-to-market, improving cycle times and decision-making, strengthening organisational commitment, and building sustainable competitive advantage (Davenport and Prusak, 1998)"³¹⁷.

Snowden's position on KM is one where he views it as having existed in three ages³¹⁸. As such he offers outlines of KM as perceived in each age. Snowden's outlines are structured around the perception of knowledge, its use and application in organisations and knowledge flows. Snowden states that the first age, before 1995, sees knowledge being managed with "the focus being on the appropriate structuring and flow of information to decision-makers and the computerisation of major business applications, leading to a technology-enabled revolution dominated by the perceived efficiencies of process reengineering"³¹⁹. According to Snowden,

³¹¹ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

³¹² Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

³¹³ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

³¹⁴ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 5.

³¹⁵ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

³¹⁶ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

³¹⁷ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4.

³¹⁸ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

³¹⁹ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

the problem with this approach was that organisations were starting to recognise that they might have achieved efficiencies at the cost of effectiveness³²⁰. Snowden explains this meant that key experience and knowledge was lost which compromised the effectiveness of their business operations leading to the concept of knowledge becoming problematic.

They had laid off people with experience or natural talents, vital to their operation, of which they had been unaware... They failed to recognise the value of knowledge gained through experience, through traditional forms of knowledge transfer such as apprentice schemes, and the collective nature of much knowledge, was such that the word knowledge became problematic³²¹.

The transition to the second age took place around 1995, with the emergence of the term KM³²². This was driven forward by the popularisation of the Socialisation, Externalisation, Combination, and Internalisation (SECI) model developed by Nonaka and Takeuchi³²³, with its focus on the movement of knowledge between tacit and explicit states through the four processes of SECI³²⁴. The misunderstanding by professionals following the SECI model was one of segmenting tacit and explicit knowledge as two distinct knowledge elements isolated from one another³²⁵. Snowden points out that the concept of tacit and explicit knowledge was not new, having had its roots in the work of Polanyi³²⁶, but with one key difference to the way it was understood and implemented by knowledge professionals.

Where Polanyi saw tacit and explicit as different but inseparable aspects of knowledge, the de facto use of the SECI model was dualistic, rather than dialectical... Nonaka attempted to restate his more holistic and dialectical view of tacit and explicit knowledge when he republished the model utilising the Japanese word “Ba”, which is a “Shared space for emerging relationships” (Nonaka & Konno 1998), but by this time the simple two by two of the SECI model was too well established in business plans, software brochures and the structured methods of consultants to be restored to its original intent³²⁷.

³²⁰ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

³²¹ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

³²² Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

³²³ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

³²⁴ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

³²⁵ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 3.

³²⁶ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2.

³²⁷ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2-3.

For example, Nonaka and Takeuchi view KM in organisations as an enabling factor³²⁸, which takes place through a process of tacit and explicit feedback and exchange. What many professionals seemed to miss was that as Nonaka and Takeuchi stated “the creation of new knowledge is not simply a matter of *processing* objective information”³²⁹. It is rather a result of this tacit-explicit relationship in the context of the organisation and how organisations make use of this resource.

... it rather depends on tapping the tacit and often highly subjective insights, intuitions, and hunches of individual employees and making those insights available for testing and use by the company as a whole³³⁰.

As Serban and Luan state, Nonaka and Takeuchi have reasoned that “structured or codified building blocks are explicit knowledge whereas unstructured, difficult-to-codify building blocks are tacit knowledge”³³¹. Organisations from this perspective are entities that can use knowledge to their benefit, for the process of self-renewal³³², by drawing on these tacit and explicit exchanges to innovate and gain competitive advantage.

For the third age of KM, Snowden takes a more informal systematic view. This is one arising due to the perceptions of KM being challenged³³³. Snowden views the third age of KM as based on three different types of informal systems, these being: complicated, complex, and chaotic systems. Snowden encapsulates this position in his Cynefin model, where he examines how knowledge flows through a process of chaos to complexity, from the knowable with a branch to known and then back to chaos³³⁴. Snowden advises that what this means for organisations in the third age of KM is that they need to realise their dependence on informal networks, rather than centrally structured approaches to managing knowledge³³⁵. He explains this as a shift from second-generation KM to third-generation KM and the creation of just in time knowledge ecologies. Knowledge is thus seen to be much more of a dynamic entity rather than as the result of rigid business processes.

³²⁸ Nonaka & Takeuchi, 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* p 60.

³²⁹ Nonaka, 1991. *The Knowledge Creating Company* p 97.

³³⁰ Nonaka, 1991. *The Knowledge Creating Company* p 97.

³³¹ Serban & Luan, 2002. *Overview of Knowledge Management* p 9.

³³² Nonaka, 1991. *The Knowledge Creating Company* p 96-97.

³³³ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 2-7.

³³⁴ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 7.

³³⁵ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 11.

For many years stock was held on the factory floor in anticipation of need at a high cost and risk of redundancy. Eventually it was realised that this was a mistake and significant levels of stock were pushed back to suppliers entering the factory on the just in time basis thus minimising costs. Second-generation knowledge management made all the same mistakes. In the third generation we create ecologies in which the informal communities of the complex domain can self-organise and self-manage their knowledge in such a way as to permit that knowledge to transfer to the formal, knowable domain on a just in time basis³³⁶.

Müller³³⁷ explains that how knowledge has been viewed in organisations has brought about corrections in perceptions and framing of knowledge. According to Müller³³⁸, this has resulted in the manifestation of these different phases. It is also important to note that each phase is in contest with the other and that one phase does not necessarily follow on from the next³³⁹. From this view, Davenport, Cronin and Tuomi have outlined the evolution of KM³⁴⁰ as comprising of these three distinct phases.

Davenport and Cronin view the first phase of KM as being synonymous with information management³⁴¹. From their perspective, this can be thought about as the management of internal and external publications³⁴² through various technical or non-technical mechanisms. The second phase of KM is viewed as KM contextualised through an organisation's business processes and activities, with a strong focus on ontologies of activities and capabilities³⁴³. In other words, the management of an organisation's "know-how"³⁴⁴. The third phase of KM as seen by the authors is one with a focus on knowledge as a capability rather than a resource³⁴⁵. From this perspective, KM allows an organisation to use knowledge to respond³⁴⁶ to various

³³⁶ Snowden, 2002. *Complex Acts of Knowing: Paradox and Descriptive Self-Awareness* p 7.

³³⁷ Müller, 2014. *Knowledge Management*.

³³⁸ Müller, 2014. *Knowledge Management*.

³³⁹ Müller, 2014. *Knowledge Management*.

³⁴⁰ Tuomi, 2002. *The Future of Knowledge Management* p 69.

³⁴¹ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁴² Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁴³ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁴⁴ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁴⁵ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁴⁶ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

challenges as they arise in the business environment. Doing so allows organisations to co-evolve effectively with and within a given environment³⁴⁷.

Building on this perspective, Tuomi outlines what he calls the three generations of KM³⁴⁸. According to Tuomi³⁴⁹, first-generation KM is a clustering of different approaches, rather than one well defined and integrated KM discipline. From this position, knowledge is seen as something that can be captured, stored, and managed using software and information systems³⁵⁰. This is like Davenport and Cronin's first phase KM, where it is focused on information management activities³⁵¹ and where knowledge is seen more as a tangible resource.

From Tuomi's perspective, second-generation KM differs from the first generation in that it focuses on the emergence of the KM specialist³⁵². In this generation, KM activity is combined and absorbed into everyday organisational discourse through tools like social learning and communities of practice (COPs)³⁵³. It means that organisations view knowledge as something that can be extended beyond the realm of information systems and software to include centralised sharing³⁵⁴. This differs from Davenport and Cronin's view of second phase KM, in that Tuomi's second generation of KM is seen to be less driven by ontologies³⁵⁵. Rather it is seen more as the centralisation of KM, as a managed and integrated organisational activity.

Tuomi views the third generation of KM as focused on the collective social understanding of knowledge³⁵⁶, rather than as a centrally managed and shared entity. Firestone and McElroy³⁵⁷ argue that collective social understanding is achieved through the interactions that take place in the dynamics of organisational culture. This means that interaction is the primary modus for creating knowledge and innovation³⁵⁸. Achieving this is done through sense-making processes that are framed by the collective culture of the organisation³⁵⁹. It is thus logical to assume that

³⁴⁷ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁴⁸ Tuomi, 2002. *The Future of Knowledge Management* p 69.

³⁴⁹ Tuomi, 2002. *The Future of Knowledge Management* p 79.

³⁵⁰ Tuomi, 2002. *The Future of Knowledge Management* p 71.

³⁵¹ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁵² Tuomi, 2002. *The Future of Knowledge Management* p 79.

³⁵³ Tuomi, 2002. *The Future of Knowledge Management* p 79.

³⁵⁴ Firestone & McElroy, 2005. *Doing Knowledge Management*. p 11-17.

³⁵⁵ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁵⁶ Tuomi, 2002. *The Future of Knowledge Management* p 79.

³⁵⁷ Firestone & McElroy, 2005. *Doing Knowledge Management*. p 11-17.

³⁵⁸ Firestone & McElroy, 2005. *Doing Knowledge Management*. p 11-17.

³⁵⁹ Firestone & McElroy, 2005. *Doing Knowledge Management*. p 11-17.

if KM is engrained in an organisation's collective culture it will, as a by-product, become more effective at adapting to a changing business environment.

Viewed in this way, it is like Davenport and Cronin's view of third phase KM, in that they highlight the shift of knowledge from an organisational resource to knowledge as an organisational capability³⁶⁰. Using KM as an organisational capability allows an organisation to adapt strategically to the needs of its environment by using its collective knowledge. Kulkarni³⁶¹ suggests that the strategic use of KM in this instance takes place when pursuing the purpose of increased innovation, using knowledge, to gain competitive advantage in some way.

Knowledge Management (KM) is evolving into a strategically important area for most organizations. Broadly, KM can be viewed as the process by which organizations leverage and extract value from their intellectual or knowledge assets. Knowledge has been described as information combined with experience, context, interpretation, and reflection [19]. Knowledge is embedded and flows through multiple entities within a firm, including individuals with domain expertise, specific best-known methods, or lessons learned from similar experiences, documents, routines, systems, and methods³⁶².

These key theoretical positions help to provide context as to the development and meaning of KM activities in organisations. They will also be useful when it comes to analysing why and how to frame knowledge security as a KM problem conceptually. However, using them to solidify a definition of KM is a trickier task. This is due to several factors which will be outlined in the section to follow.

3.4 The Problem with Defining Knowledge Management

As in the case of defining knowledge, it is also difficult to achieve consensus when defining KM. Davenport and Cronin³⁶³ argue that even though there has been a large amount of academic attention given to KM, it is still not an area that is unified around a singular approach.

³⁶⁰ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁶¹ Kulkarni *et al.*, 2006. *A Knowledge Management Success Model: Theoretical Development and Empirical Validation* p 310.

³⁶² Kulkarni *et al.*, 2006. *A Knowledge Management Success Model: Theoretical Development and Empirical Validation* p 310.

³⁶³ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

In addition, from a professional perspective³⁶⁴, Bolisani³⁶⁵ explains that there is also not a unified approach to KM followed by companies. This is because each of them chooses those tools and solutions that they deem to be useful for their needs³⁶⁶. This makes it a difficult task to provide a definition of consensus regarding KM from the literature. The complexity in defining KM, as hinted at here, rests with several contributing factors.

Firstly, as explained by Terra and Angeloni³⁶⁷, there is little consensus when it comes to defining KM. From their perspective, this lack of consensus arises from KM being premised on an already fragmented concept, that of knowledge and its definitions³⁶⁸. As seen in Chapter 2, defining organisational knowledge is not easy to do. This is because knowledge can be a solidified or abstract concept that can carry a lot of different meanings, depending upon how it is applied and in what context it is used.

Secondly, as stated in the previous section, KM has arisen from multiple disciplines³⁶⁹. The varying nature of these different disciplines has further added to the complexity of understanding³⁷⁰ and thus defining KM. When thinking of definitions of KM with this background in mind, it could be argued that an additional layer of complexity is added in interpreting KM as part of organisational processes. One aspect of KM might be thought of as more important to emphasise than another depending on the context it is defined in. Thus, selecting a definition and focus relating to KM becomes dependant on sensemaking processes. How KM is framed and interpreted will determine how it is defined and implemented as part of the intersection between individuals, their environment, and organisational processes³⁷¹. Considering when it is combined with each organisation's unique set of requirements, the background of the practitioners who implement it and the way it is framed in accordance with the organisation's objectives.

³⁶⁴ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

³⁶⁵ Bolisani *et al.*, 2015. *How Small KIBS Companies Manage their Intellectual Capital? Towards an Emergent KM Approach* p 31.

³⁶⁶ Bolisani *et al.*, 2015. *How Small KIBS Companies Manage their Intellectual Capital? Towards an Emergent KM Approach* p 31.

³⁶⁷ Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2.

³⁶⁸ Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2.

³⁶⁹ Serban & Luan, 2002 *Overview of Knowledge Management* p 6-7.

³⁷⁰ Serban & Luan, 2002 *Overview of Knowledge Management* p 6-7.

³⁷¹ Mills *et al.*, 2010. *Making Sense of Sensemaking: The Critical Sensemaking Approach* p 182-196.

Thirdly, KM is also a concept that is constantly evolving³⁷² and is thus associated with a certain degree of change in the way organisations have viewed and applied KM activities over time. With the rise in the importance of information and knowledge as key commodities³⁷³, organisations have grappled with understanding how to effectively manage these commodities. This has meant a growing list of management areas or ‘enthusiasms’ associated with KM³⁷⁴, either as precursors to it, or that have now been incorporated under the umbrella term of KM³⁷⁵. Thus, KM has often been associated with and presented similarly to ‘fad like’ management approaches³⁷⁶, further increasing confusion. This has added even more complexity when trying to identify an accepted type of KM or provide a common definition, especially when combined with knowledge and the original collection of disciplines that make up KM.

Though considerable academic and professional attention has been focused on this area in the past decade, the concept is not yet stable: the term appears to be used differently across domains with each claiming that its partial understanding represents a definitive articulation of the concept...³⁷⁷

Thus, my objective is to outline and consolidate the various common KM definitions from the literature. I will do this to find commonalities in the definitions and select a definition that is representative of the most common KM views. Having a clear perspective on this will assist with analysing the need to integrate knowledge security as part of KM conceptually. It will also assist with helping to provide context to any KM frameworks used in later chapters.

3.5 Consolidating Definitions of Knowledge Management

As seen in the previous section, some issues make defining KM from a singular perspective difficult. This is evident by the broad array of definitions of KM that can be found in the literature. Girard and Girard point out that the scope of KM is overly broad and deep, with more than 100 definitions included in their analysis of KM definitions from an array of different

³⁷² Courtney, 2001. *Decision Making and Knowledge Management in Inquiring Organisations: Toward a New Decision-Making Paradigm for DSS* p 20.

³⁷³ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1-2.

³⁷⁴ Koenig, 2018. *What is KM? Knowledge Management Explained* [Online].

³⁷⁵ Koenig, 2018. *What is KM? Knowledge Management Explained* [Online].

³⁷⁶ Fotache, 2005. *Knowledge Management: Between Fad and Relevance* p 266.

³⁷⁷ Davenport & Cronin, 2000. *Knowledge Management Semantic Drift or Conceptual Shift?* p 294.

disciplines³⁷⁸. Thus, attempting to cover all the possible definitions of KM is not a realistic task for this study.

In selecting a definition of KM, there are two primary ways to approach this problem. Firstly, I can adopt a definition of KM that is representative of the broader body of definitions. This can be done either through an integrated definition or through a consolidation process. Secondly, I may select a definition that is not necessarily representative, but one that I decide can be justified by its selection when compared to other KM definitions. Considering these options, I will select the first approach to choosing a KM definition. The definition will be derived from a process of consolidation.

My reason for choosing this approach is that while there are general similarities concerning the idea of sharing knowledge in the definitions, there is not a comprehensive consensus on what approaches to include or how to frame all aspects in one definition. Therefore, my justification for doing so is that since there is such a broad array of definitions, it would be better to have more breadth as to what is common amongst them. Regarding not using an integrated approach, initially when examining definitions of KM, I did attempt to do this. However, I found that it was difficult to keep the definitions representative enough without becoming cumbersome. I also found that it was difficult to include all the key perspectives from the literature and include all of them in the argument. As a result, I found the scholarly merit of that approach to be weaker. This is also why I chose not to single out one KM definition, and argue for its merits, without considering a larger sample of the body of definitions in the literature.

In their paper on defining KM³⁷⁹, Girard and Girard end by offering a consolidated definition of KM comprised of the most prominent keywords found in their analysis. These keywords have been aggregated from their list of more than 100 KM definitions³⁸⁰ into a definition of KM that is representative of the most common terms. Their two consolidated definitions of KM are outlined as follows.

Knowledge Management is the process of creating, sharing, using and managing the knowledge and information of an organization... Knowledge Management is the

³⁷⁸ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 2.

³⁷⁹ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 14.

³⁸⁰ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 14.

management process of creating, sharing and using organizational information and knowledge³⁸¹.

To validate their definition, I chose to conduct a sample study of between 20-30 prominent definitions from the literature and replicate Girard and Girard's approach. This was done to see if I would get similar results as derived from their methodology or if any aspects were missing.

The methodology followed by Girard and Girard³⁸² was to first compile their list of definitions from predominantly open sources. Next, they used a word parsing tool to create a list of common words. They eliminated the word combination "knowledge management" from their list of definitions. They did this to ensure that the emphasis remained on individual words and so as not to exaggerate the words knowledge and management. They also grouped root word combinations to eliminate the redundancy of terms. They removed all prepositions and pronouns as they were not the focus of the analysis. Finally, words that appeared at least four times were included on their initial list of words. To cut those down they chose the most common words, those which appeared 30 times or more. These words they then used to create their consolidated definitions of KM. I followed the same approach with my smaller analysis.

Firstly, I chose to compile a list of between 20-30 definitions. This offered enough scope to include what I perceived as the most prominent definitions of KM as found in the academic literature. I ended with a sample size of 22 definitions, with 6 of them overlapping Girard and Girard's list. I applied the same process by removing the word combination "knowledge management", grouping root words, removing prepositions and pronouns, and filtering the output for the most common terms. My list of definitions chosen from the academic literature is presented in Table 3-3, with the duplicate definitions being indicated as such.

Following the compilation of this list, I analysed the definitions as per Girard and Girard's filtered approach³⁸³ and by using a word parsing tool. Next, I listed my words in a table to cross-reference my results with that of Girard and Girard. The idea was that the comparison would indicate to me if I could adopt their definition of KM or if another approach were needed. Girard and Girard's analysis found that the most common words, which appeared over 30 times³⁸⁴ (29.41%), were the words: knowledge (112); organisation (69); process (50);

³⁸¹ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 13.

³⁸² Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 13.

³⁸³ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 2.

³⁸⁴ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 13.

Table 3-3: List of KM Definitions Chosen from the Academic Literature

Author	Definition
Davenport	The process of capturing, distributing and effectively using knowledge ³⁸⁵
Wiig	An activity that has the intention to manage knowledge practically and effectively to reach broad operational and strategic objectives ³⁸⁶
Skyrme (duplicate)	The explicit and systematic management of vital knowledge and its associated processes of creating, gathering, organising, diffusion, use and exploitation. It requires turning personal knowledge into corporate knowledge that can be widely shared throughout an organisation and appropriately applied ³⁸⁷
Beckman	The formalisation of, and access to, experience, knowledge and expertise that create new capabilities, enable superior performance, encourage innovation, and enhance customer value ³⁸⁸
Murray & Myers	The collection of processes that govern the creation, dissemination, and utilisation of knowledge to fulfil organisational objectives ³⁸⁹
Davenport and Prusak (duplicate)	Drawing from existing resources that your organization may already have in place-good information systems management, organizational change management, and human resources management practices ³⁹⁰
Von Krogh	A process of identifying, capturing, and leveraging the collective knowledge in an organisation to help the organisation compete ³⁹¹
Duhon	A discipline that promotes an integrated approach to identifying, capturing, evaluating, retrieving, and sharing all of an enterprise's information assets ³⁹²

³⁸⁵ Davenport, 1994. *Saving ITs Soul: Human Centred Information Management* p 119-131.

³⁸⁶ Wiig, 2000. *Knowledge Management: An Emerging Discipline Rooted in a Long History* p 6.

³⁸⁷ Skyrme, 1997. *Knowledge Management – Making Sense of an Oxymoron* p 6.

³⁸⁸ Beckman, 1997. *A Methodology for Knowledge Management* p 1-6.

³⁸⁹ Murray & Myers, 1997. *The Facts About Knowledge* p 29.

³⁹⁰ Davenport & Prusak, 1998. *Working Knowledge: How Organizations Manage What They Know* p 163.

³⁹¹ von Krogh, 1998. *Care in Knowledge Creation* p 133-153.

³⁹² Davenport, 1994. *Saving ITs Soul: Human Centred Information Management* p 119-131.

Author	Definition
O'Dell <i>et al.</i> (duplicate)	A conscious strategy of getting the right knowledge to the right people at the right time and helping people share and put information into action in ways that strive to improve organisational performance ³⁹³
Preston <i>et al.</i>	Any process or practice of creating, acquiring, capturing, sharing, and using knowledge, wherever it resides, to enhance learning and performance in organisations ³⁹⁴
Alavi & Leidner	The systematic and organisationally specified process of acquiring, organising, and communicating knowledge of employees so that other employees may make use of it to be more effective and productive in their work ³⁹⁵
Davenport & Prusak	A fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information ³⁹⁶
Mårtensson	The management of the “intellectual capital” controlled by the company ³⁹⁷ ... and the acquisition and storage of workers’ knowledge and making information accessible to other employees within the organisation ³⁹⁸
Thomas, <i>et al.</i>	A problem of capturing, organising, and retrieving information, evoking notions of databases, documents, query languages, and data mining ³⁹⁹
Watson	Something treated broadly and is used to cover all that an organisation needs to know to perform its functions ⁴⁰⁰

³⁹³ O'Dell *et al.*, 1998. *If Only we Know What we Know: The Transfer of Internal Knowledge and Best Practice* p 4.

³⁹⁴ Preston *et al.*, 1999. *Knowledge Management – A Literature Review* p 88.

³⁹⁵ Alavi & Leidner, 1999. *Knowledge Management Systems: Issues, Challenges, and Benefits. Communications of the AIS* p 1-38.

³⁹⁶ Dieng & Corby (Eds.), 2000. *Knowledge Engineering and Knowledge Management: Methods, Models, and Tools* p 1-457.

³⁹⁷ Mårtensson, 2000. *A Critical Review of Knowledge Management as a Management Tool* p 205.

³⁹⁸ Mårtensson, 2000. *A Critical Review of Knowledge Management as a Management Tool* p 205.

³⁹⁹ Thomas *et al.*, 2001. *The Knowledge Management Puzzle: Human and Social Factors in Knowledge Management* p 863–884.

⁴⁰⁰ Watson, 2002. *Applying Knowledge Management: Techniques for Building Corporate Memories* p 4.

Author	Definition
Holsapple	Less to do with the relatively trivial operational issues of collecting, sorting, and communicating data, even in the vastly greater quantities that now seem both possible and necessary, than with a new impetus to examine and perhaps, manage the meaning and context of our work and organisational activity ⁴⁰¹
Frost (duplicate)	The systematic management of an organisation's knowledge assets for the purpose of creating value and meeting tactical and strategic requirements; it consists of the initiatives, processes, strategies, and systems that sustain and enhance the storage, assessment, sharing, refinement, and creating of knowledge ⁴⁰²
Ogrean	Managing the processes that act upon knowledge assets, and these processes include: developing knowledge; preserving knowledge; using knowledge, and sharing knowledge ⁴⁰³
Snowden (duplicate)	Something to provide support for improved decision making and innovation throughout the organization. This is achieved through the effective management of human intuition and experience augmented by the provision of information, processes, and technology together with training and mentoring programmes ⁴⁰⁴
Milton (duplicate)	As the way you manage with due attention to the value of knowledge ⁴⁰⁵
Young	As the discipline of enabling individuals, teams, and entire organisations to collectively and systematically create, share and apply knowledge, to better achieve their objectives ⁴⁰⁶
Becerra-Fernandez & Sabherwal	Simply doing what is needed to get the most out of knowledge resources ⁴⁰⁷

⁴⁰¹ Holsapple (Eds), 2002. *Handbook on Knowledge Management 1: Knowledge Matters* p 60-61.

⁴⁰² Frost, 2010. *Knowledge Management Definition* [Online].

⁴⁰³ Ogrian, 2006. *Knowledge Management – A Source of Sustainable Competitiveness in the Knowledge Based Economy* p 7.

⁴⁰⁴ Snowden, 2009. *Defining Knowledge Management* [Online].

⁴⁰⁵ Milton, 2009. *What is Knowledge Management?* [Online].

⁴⁰⁶ Young, 2010. *Knowledge Management and Innovation in a Global Knowledge Economy* p 17.

⁴⁰⁷ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 4-5.

information (44); use (40); share (36); create (33); manage (30)⁴⁰⁸. Using the same method, the following words appeared most often in my list: knowledge (22); organisation (18); manage (11); process (10); information (8); create (7); share (7). These are words that appear over 6.47 times (29.41%). A comparison of the results of the two analyses lists is provided in Table 3-4.

Table 3-4: A Comparison of the Most Common Words Relating to KM Definitions

Results of Girard & Girard's Analysis	Results of my Analysis
Knowledge (112)	Knowledge (22)
Organisation (69)	Organisation (18)
Process (50)	Manage (11)
Information (44)	Process (10)
<i>Use (40)</i>	Information (8)
Share (36)	Create (7)
Create (33)	Share (7)
Manage (30)	

Although appearing in a different order, all but one of the words appear on my common KM definition word list too; the exception being the word *use (40)*. The omission of this word from my list and the difference in the ordering of the lists can be explained by the smaller sample size of my list. In addition, I also focused less on open-source KM definitions and obtained my definitions from academic literature such as books, journals, etc. Thus, definitions were included in my list that potentially have a different focus to some of those included in Girard and Girard's list. For all intents and purposes, they comprise mostly the same list of words.

Therefore, given the similarities in our lists, for this research, it is safe to say that Girard and Girard's definition of KM is adequately representative of the broader commonalities found in the literature. Concerning the format of their consolidated definitions, the second one "knowledge management is the management process of creating, sharing, and using organizational information and knowledge"⁴⁰⁹, seems to make the most sense for my purpose.

⁴⁰⁸ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 13.

⁴⁰⁹ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 13.

This is due to subtle differences in the phraseology of the definitions. Firstly, in my opinion, the phrase “the management process” emphasises the management orientated process-driven nature of KM⁴¹⁰ more than using the phrase “the process”. Examining KM processes will be an important aspect to consider when looking at KM from a security perspective, in terms of how to integrate knowledge security with KM conceptually. Secondly, using the phrase “organizational information and knowledge” rather than “knowledge and information of an organization” implies a broader scope as to where knowledge resides and in what capacity it can impact the organisation.

3.5.1 Limitations of the Approach

While it is useful to analyse the broad array of definitions in this manner, the process is not without limitation. In terms of developing a consolidated definition, there exist some limitations with certain aspects of the methodology used. Girard and Girard⁴¹¹ explain that the major methodological limitation of their approach was with the collecting of the definitions. As they outline, they only made use of definitions that were easily accessible on the Internet⁴¹². Thus, as they state concerning the definitions selected, “the collection should be considered a convenience sample”⁴¹³. In addition, there was no attempt made to include every definition penned and all the definitions were given in English⁴¹⁴.

From my approach, there were also some limitations. Firstly, as this was just a sample examination, my list of definitions was much smaller than Girard and Girard’s as indicated earlier. Secondly, as I had six overlapping definitions in my sample, it can be argued that it would contribute to finding the same common terms as Girard and Girard did. While I did consider this aspect, and the possibility of excluding some definitions, I decided not to. I retained them because these definitions represent some of the fundamental definitions of KM from the academic literature. Leaving them out, it can be argued, could have skewed the results in other directions, not relevant to KM. Therefore, I believe the compromise of still including them to be valid and the definition adopted appropriate.

⁴¹⁰ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 41.

⁴¹¹ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 2.

⁴¹² Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 2.

⁴¹³ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 2.

⁴¹⁴ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 2.

3.6 Conclusion

Chapter 3 formed the second part of the theoretical analysis and aimed at outlining how the key theoretical issues and positions in the literature relate to KM, how KM can be defined, and why there is a need to integrate knowledge security and KM. This was in line with the research questions as illustrated in Figure 1-2⁴¹⁵ ⁴¹⁶. Thus, the objective of Chapter 3 was to add clarity by offering a consolidated definition of KM. This was done by reviewing the literature by firstly examining the rise in importance of KM to set the context. Building on this context, the literature was then examined further to outline the key theoretical positions in KM. I did so as a precursor to examining definitions of KM. Next, a discussion was held concerning the problems associated with defining KM. Finally, a solution was provided to these problems in the form of the selection of a consolidated definition of KM. Forming the final part of the theoretical analysis, Chapter 4 will examine the security literature to establish key security concepts. The objective of doing so will be to determine what security dimensions are expressed therein while keeping the KM paradigm in mind. This pertains to the research objectives of examining what security approaches are expressed in the literature that focus on KM, how they can be categorised, and why there is a need for knowledge security.

⁴¹⁵ Research sub-question 3.1: *What are the key theoretical issues and positions in the literature as they relate to KM and how can it be defined?*

⁴¹⁶ Research sub-question 3.2: *Why is there a need to integrate knowledge security with KM?*

Chapter 4

Literature Review of Knowledge Security Approaches

4.1 Introduction

In this chapter, I review the security literature and examine what security approaches are expressed therein, keeping the KM paradigm in mind. Firstly, to add context, I begin by outlining why there is a need to integrate knowledge security with KM and why there is a need for knowledge security in organisations. Next, through a literature review and categorisation process, I establish the core paradigms and perspectives as they relate to knowledge security. Using this as a base, I then proceed to outline the key perspectives according to their general thematic paradigms. I did this as a precursor to Chapter 7, where the conceptual model is discussed, and the concept of knowledge security concerning KM is further refined.

4.2 The Need to Integrate Knowledge Security with Knowledge Management

With the definition of KM presented in Chapter 3 in mind, I will now outline my arguments as to why there is a need to integrate knowledge security with KM. The arguments in favour of aligning knowledge security with KM will be outlined in two primary streams. Firstly, that there is a difference between information and knowledge, and that this difference echoes into how information and knowledge are handled in organisations. This can be seen in terms of the requirements for managing and securing information and knowledge. Secondly, that organisational knowledge has value and as such should be secured in a way that is far-reaching enough to deal with the unique challenges of KM; something which, as I will argue, information security cannot always do.

To begin, in contrast with defining organisational knowledge and its associated complexities, as outlined in Chapter 2, defining organisational information is more straightforward. Terra and Angeloni state that generally “definitions of information tend to be far more uniform and

less complex than definitions of knowledge”⁴¹⁷. Definitions of information also tend to be more thematic⁴¹⁸. Often, they are themed as information defined as being meaning derived from codifying and interpreting data⁴¹⁹. Or they are themed as information defined as an entity, through a process of codification, which can tangibly transfer its meaning⁴²⁰.

For example, when examining definitions of information from the literature, Probst *et al.* define information as “interpreted data”⁴²¹, data codified in some way that requires some level of interpretation. Drucker defines information as “data empowered with relevance and purpose”⁴²² and as such, once empowered, its meaning may exist without additional human input. Saint-Onge defines information as “organised data”⁴²³, again echoing the codified nature of information. Davenport defines information as “data with relevance and purpose”⁴²⁴, which hints at information as being codified and interpreted data whose meaning has value and applicability in a relevant situation. Wiig defines information as “facts organised to describe a situation or condition”⁴²⁵, thus still hinting at the contained and encoded meaning derived from the ability of information to describe something. Continuing this idea, further definitions from the literature focus on this component and the conveyance of meaning through the transferability of information.

From this perspective, Nonaka and Takeuchi define information as “a flow of meaningful messages”⁴²⁶, hinting at the transfer of tangible data compiled in a meaningful way. Spek and Spijkervet define information as “data with meaning”⁴²⁷, further supporting the view of

⁴¹⁷ Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2-3.

⁴¹⁸ Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2-4.

⁴¹⁹ Zins, 2007. *Conceptual Approaches for Defining Data, Information, and Knowledge* p 481.

⁴²⁰ Zins, 2007. *Conceptual Approaches for Defining Data, Information, and Knowledge* p 481.

⁴²¹ Probst *et al.* cited in Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2.

⁴²² Drucker cited in Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2.

⁴²³ Saint-Onge cited in Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2.

⁴²⁴ Davenport cited in Stenmark, 2002. *Information vs. Knowledge: The Role of Intranets in Knowledge Management* p 929.

⁴²⁵ Wiig, 1994. *Knowledge Management Foundations: Thinking About Thinking – How People and Organizations Create, Represent, and Use Knowledge* p 2.

⁴²⁶ Nonaka & Takeuchi, 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* p 60.

⁴²⁷ Spek & Spijkervet, 1997. *Knowledge Management: Dealing Intelligently with Knowledge*.

information as something which users derive meaning from when compiled data is interpreted. Choo *et al.* define information as “data vested with meaning”⁴²⁸, alluding to information as a collection of data that has been compiled and interpreted in some way to derive its meaning. Thus, information is something that does not rely on the same level of human-driven tacit/explicit relationship and associated contextual factors for the development of its meaning. Rather that meaning is contained in a transferrable, codified form which may or may not be interpreted further.

Given these differences, the difference between information and knowledge also alludes to the difference in the role of necessary human interaction for the successful management of each entity. While information, and the way it is created and processed, relies on human participation to some degree for its success⁴²⁹, individuals play a far more critical role when it comes to creating and processing knowledge⁴³⁰. Knowledge relies heavily on deduction, socialisation processes, the application and generalisation of understanding and the interplay between individuals in contexts around tasks⁴³¹, as outlined by Terra and Angeloni below:

The key difference can be summarized by the role played by human beings. In the case of knowledge, as simple as it may seem, individuals play a prominent role as creators, carriers, conveyors and users. In contrast, in the case of information, these same functions can happen “outside” humans and without their direct influence⁴³².

The echoing effect of this difference can also be seen in the way information and knowledge are managed in organisations. While having some level of overlap in the use of technology, information management at its core has a different set of requirements to KM⁴³³. The Association for Intelligence Information Management (AIIM)⁴³⁴ advises that information includes both electronic and physical information. The goal in this instance is to structure the organisation so it can manage this information throughout its life cycle⁴³⁵, regardless of the

⁴²⁸ Choo *et al.*, 2000. *Web Work: Information Seeking and Knowledge Work on the World Wide Web*.

⁴²⁹ Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2-3.

⁴³⁰ Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 3-4.

⁴³¹ Tsoukas & Vladimirou, 2002. *What is Organisational Knowledge* p 973.

⁴³² Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 3-4.

⁴³³ AIIM, 2019. *What is Information Management?* [Online].

⁴³⁴ AIIM, 2019. *What is Information Management?* [Online].

⁴³⁵ Virtue & Rainey, 2015. *Information Risk Assessment* p 133-166.

source or format of that information⁴³⁶. The purpose of this structuring is to provide access to information resources when needed; mostly through electronic means⁴³⁷. While KM may include the use of information technologies to actualise its objectives, it may also use socialisation, sense-making and decision-making processes, which are less rigid compared to information management processes.

Based on these views, it can also be argued that the approaches used to securing information will not be able to deal with all the complexities that are involved in securing knowledge. Without going into detail, as this will be discussed in Chapter 4, information security focuses mainly on securing those electronic and physical forms of information that exist within an organisation⁴³⁸. Information security is enacted through eight core domains including security and risk management, asset security, security architecture and engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security⁴³⁹. The objective of these domains is to ensure the confidentiality, integrity, and availability (CIA) of an organisation's information.

From an information security perspective confidentiality involves providing access to information only to those individuals who are authorised to do so⁴⁴⁰. Integrity involves ensuring that information is not altered by anyone unauthorised to do so⁴⁴¹. Availability involves ensuring that information is available when needed⁴⁴². CIA also forms the basis of most data protection legislation and industry standards in information security⁴⁴³.

Even though information security is certainly useful to securing knowledge where information and communication technologies (ICTs) are used, I would argue that in the other aspects of KM, information security does not extend far enough. Melnick states that "KM is not all about

⁴³⁶ AIIM, 2019. *What is Information Management?* [Online].

⁴³⁷ AIIM, 2019. *What is Information Management?* [Online].

⁴³⁸ Warwick University, 2019. *Information and Data Compliance - Quick Guide to Information Security at Warwick* p 3.

⁴³⁹ Chapple *et al.*, 2018. *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide* p xxxiii.

⁴⁴⁰ Warwick University, 2019. *Information and Data Compliance - Quick Guide to Information Security at Warwick* p 1-3.

⁴⁴¹ Warwick University, 2019. *Information and Data Compliance - Quick Guide to Information Security at Warwick* p 1-3.

⁴⁴² Warwick University, 2019. *Information and Data Compliance - Quick Guide to Information Security at Warwick* p 1-3.

⁴⁴³ Warwick University, 2019. *Information and Data Compliance - Quick Guide to Information Security at Warwick* p 3.

technology. Instead, it involves both information management (technology) and knowledge-building (people)”⁴⁴⁴. Thus, the unique factors needed to secure organisational knowledge need to be considered. This is because the risks arising from KM processes extend beyond the realms of tangible information assets and technical systems. For example, information security domains would not be able to deal with the impact of an organisation not having knowledge retention or learning strategies. They would not be able to deal with the risks posed by informal cross-departmental or organisational social interaction and sharing. They would not be able to deal with the knowledge security risks created by the resistance of employees to adopting a KM initiative and the impact on innovation. Thus, a different approach to securing knowledge assets is needed, one that aligns with KM processes. Knowledge security would be better positioned as something aligned with KM to recognise and handle these challenges.

An additional issue is the lack of integration of information systems security with KM^{445 446}, even though information systems security overlaps with knowledge security in some respects. Jennex and Durcikova⁴⁴⁷ contend that information systems security and KM should be viewed as complementary business activities, but this is currently not the case. This is evidenced by a lack of research literature addressing the integration of KM and security⁴⁴⁸. It is also evidenced by a lack of interest of practitioners in integrating KM and security⁴⁴⁹, as the authors explain in the following extract below.

The concern is that there is too little integration and that KM practitioners and researchers need to put more effort into creating secure KM (SKM). We believe this is necessary given the cyber threat environment. The cyber threat is growing... Ultimately there are persistent threats that are risks to the knowledge relied upon by our organizations. We posit that it is a responsibility of KM researchers and

⁴⁴⁴ Melnick, 2007. *Using KM Principles to Drive Productivity and Performance, Prevent Critical Knowledge Loss and Encourage Innovation* p 17.

⁴⁴⁵ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁴⁶ Becerra-Fernandes & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 10.

⁴⁴⁷ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁴⁸ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁴⁹ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

practitioners to develop secure KM so that these critical knowledge assets can be stored, accessed, and utilized⁴⁵⁰.

This is a risk because, as Jennex and Durcikova⁴⁵¹ state, “knowledge has value and items of value are targets of theft and attack”. There is an ever-increasing growth in cyber-attacks and espionage when it comes to IP, with knowledge being a key component of IP⁴⁵². This risk is compounded by the number of pervasive and persistent threats to the organisation coming from both insiders⁴⁵³, as well as through an ever-adapting array of technical, social, and organisational channels⁴⁵⁴ used by attackers. If KM, which deals with IP, is to be secured effectively, security processes need to be a part of the thinking behind it.

The integration of security with business or development processes is an argument that is echoed in other disciplines. For example, the mention of secure KM by Jennex and Durcikova⁴⁵⁵ relates in many ways to the call for secure coding in software development and operations. In this context, if security is not integrated as part of the development process life cycle, it can create security vulnerabilities⁴⁵⁶. Fletcher⁴⁵⁷ argues that vulnerability is lessened if security processes are integrated from the beginning of the coding life cycle. Fletcher explains further that it can also lead to less friction between security specialists and developers too⁴⁵⁸ when it comes to the balance between functionality and security⁴⁵⁹. Thus, it could be argued that there is a similar need to integrate knowledge security with KM to ensure a reduction in

⁴⁵⁰ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁵¹ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁵² Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁵³ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁵⁴ Trend Micro Research, 2019. *Mapping the Future: Dealing with Pervasive and Persistent Threats, Trend Micro Security Predictions for 2019* p 1-3.

⁴⁵⁵ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁵⁶ Vaughan-Nichols, 2019. *No Love Lost Between Security Specialists and Developers for Linux and Open Source* [Online].

⁴⁵⁷ Vaughan-Nichols, 2019. *No Love Lost Between Security Specialists and Developers for Linux and Open Source* [Online].

⁴⁵⁸ Vaughan-Nichols, 2019. *No Love Lost Between Security Specialists and Developers for Linux and Open Source* [Online].

⁴⁵⁹ Vaughan-Nichols, 2019. *No Love Lost Between Security Specialists and Developers for Linux and Open Source* [Online].

vulnerability and friction. Again, this is framed in terms of the balance needed between sharing and securing knowledge from a KM and security perspective in organisations.

4.3 The Need for Knowledge Security

In Section 4.2, I argued that the need to integrate knowledge security with KM concerns three primary issues. Firstly, the difference in the requirements for managing and securing⁴⁶⁰ information and knowledge⁴⁶¹. Secondly, the idea that knowledge has value and is something that should be protected⁴⁶². Thirdly, that there is a lack of integration of information systems security with KM⁴⁶³, even though they overlap in some respects⁴⁶⁴. A fourth point that I would like to add, as some authors have mentioned⁴⁶⁵, is that for KM to be successful in organisations, it needs to be leveraged effectively to unlock the value of organisational resources⁴⁶⁶. This is actualised through a series of critical success factors (CSFs)⁴⁶⁷, which currently do not pay much attention to knowledge security as a mechanism for unlocking that value⁴⁶⁸. When examining the need for knowledge security, it can be argued that the first three points will also be applicable from the perspective of knowledge security as well as KM. Therefore, they can be viewed as somewhat related, both theoretically and academically, when taken from the perspective of the need to integrate knowledge security with KM and to subsequently develop the concept of knowledge security too.

Relating to the first point, securing information, as opposed to knowledge, requires a different approach due to the differences between information and knowledge in organisations⁴⁶⁹ and

⁴⁶⁰ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁶¹ AIIM, 2019. *What is Information Management?* [Online].

⁴⁶² Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁶³ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁶⁴ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁶⁵ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁴⁶⁶ University of Stellenbosch, 2019. *Post Graduate Programmes in Information and Knowledge Management* [Online].

⁴⁶⁷ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁴⁶⁸ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁴⁶⁹ Terra & Angeloni, 2003. *Understanding the Difference Between Information Management and Knowledge Management* p 2.

how they are managed⁴⁷⁰. As information is more product like⁴⁷¹ existing in tangible electronic or physical forms, security is often focused on protecting these forms⁴⁷². However, securing knowledge is more difficult, as knowledge is not only found in tangible forms but intangible forms too^{473 474}. Thus, when it comes to securing organisational knowledge, the argument can be made that not all information security domains will be as effective or applicable⁴⁷⁵.

Furthermore, as Arora *et al.* outline, even in those areas where information security is applicable, as with the technical aspects of a knowledge management system (KMS), the level of complexity associated with securing that knowledge can be daunting⁴⁷⁶. This is in terms of managing permissions, roles, and access rights in a KMS as compared to an information system; drastically increasing the cognitive load placed upon IT professionals⁴⁷⁷. Additionally, organisations are also under pressure from regulatory bodies to meet compliance standards, which creates an expectation from management that knowledge will be protected⁴⁷⁸. Combine this with the need for updated security policies and practices, due to the increased demand for the accessibility and availability of such systems⁴⁷⁹, and the task becomes even more complex. The implication of this, as Arora *et al.* contend, is that it can make it almost impossible to manage the required security aspects of a KMS effectively⁴⁸⁰, resulting in the potential for increased security risk to knowledge.

⁴⁷⁰ AIIM, 2019. *What is Information Management?* [Online].

⁴⁷¹ Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 4.

⁴⁷² Warwick University, 2019. *Information and Data Compliance - Quick Guide to Information Security at Warwick* p 3.

⁴⁷³ Melnick, 2007. *Using KM Principles to Drive Productivity and Performance, Prevent Critical Knowledge Loss and Encourage Innovation* p 17.

⁴⁷⁴ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 10.

⁴⁷⁵ Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 4.

⁴⁷⁶ Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 487.

⁴⁷⁷ Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 487.

⁴⁷⁸ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 404.

⁴⁷⁹ Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 487.

⁴⁸⁰ Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 487.

Relating to the second point, that knowledge has value and should be protected⁴⁸¹, so too can the argument be made that not having a well-defined approach to securing knowledge⁴⁸², within the ever-increasing threat landscape⁴⁸³, may increase an organisation's knowledge security risk. Additionally, when framed from a practical and academic perspective, concerning the advancement of the concept of knowledge security, this point becomes even more critical. Practically, authors such as Desousa⁴⁸⁴, Jennex, and Durcikova⁴⁸⁵ argue that there is often little attention given to knowledge security in organisations. Academically, Manhart and Thalmann⁴⁸⁶ outline that research is also lacking concerning key areas when it comes to knowledge protection. The combination of these two factors creates a gap in the development of tangible approaches to securing knowledge in organisations and the theory needed to improve these tangible approaches. Thus, a situation is created where there is a resource that is of value to adversaries, yet the mechanisms needed to protect it are not fully developed.

Concerning the third point, the lack of integration of information systems security with KM⁴⁸⁷, this too is problematic due to the increase in the growth of cyber threats within the business environment⁴⁸⁸. More so, given that there are some information systems security overlaps with KM activities in certain aspects⁴⁸⁹. Thus, if relevant information systems security aspects are not applied to KM activities, it could increase the security risks facing an organisation's knowledge resources and technologies, such as a KMS. From this perspective, as Muniraman *et al.* suggest, security considerations should be integrated into the development of KMS-based solutions from the initial development and planning of such solutions and should not be an afterthought⁴⁹⁰.

⁴⁸¹ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁸² Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁸³ Trend Micro Research, 2019. *Mapping the Future: Dealing with Pervasive and Persistent Threats, Trend Micro Security Predictions for 2019* p 1-3.

⁴⁸⁴ Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 3.

⁴⁸⁵ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 5-6.

⁴⁸⁶ Manhart & Thalmann, 2015. *Protecting Organizational Knowledge: A Structured Literature Review* p 204.

⁴⁸⁷ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁸⁸ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁸⁹ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 1.

⁴⁹⁰ Muniraman *et al.*, 2007 *Security and Privacy Issues in a Knowledge Management System* p45-1-5.

Relating to the fourth point, that for KM to be successful it needs to be leveraged effectively to unlock the value of organisational resources⁴⁹¹, the importance of KM and KMSs lies in their ability to generate value and advantage for an organisation. Jennex and Zyngier contend that value comes from having something others want or do not have, while advantage comes from utilising resources better than competitors⁴⁹². For KM and KMS to be successful in an organisation, they need to be managed and leveraged to generate this value and advantage by unlocking the potential of organisational resources⁴⁹³. This can be benchmarked against a series of CSFs⁴⁹⁴ relating to the impact on business processes, strategy, leadership, efficiency, and the effectiveness of KM processes⁴⁹⁵. To determine which KM and KMS success factors are most critical, Jennex and Olfman⁴⁹⁶ synthesised the literature, according to 17 studies and 200 KM projects, down to 12 CSFs. These CSFs were then ranked according to the frequency in which they appeared in the studies and projects reviewed. Based on the 12 CSFs identified, the security or the protection of knowledge was ranked as the least commonly mentioned CSF⁴⁹⁷.

Jennex and Zyngier⁴⁹⁸ point out that of the elements put forward to measure KM success, security is also not emphasised or mentioned and in some cases is seen as a barrier to knowledge sharing. This could be explained by the larger focus in the research and practice on maximising knowledge sharing⁴⁹⁹. Ilvonen *et al.* discuss that because of this focus, less attention has been paid to other areas of KM research such as knowledge security⁵⁰⁰; which is not to say it is not an important issue. Manhart and Thalmann⁵⁰¹, Cheung *et al.*⁵⁰² and Ahmad *et al.*⁵⁰³ highlight that the detrimental consequences of ignoring knowledge protection can also include: the replication of ideas; innovation being hindered; the possibility of knowledge leaks

⁴⁹¹ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁴⁹² Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 395.

⁴⁹³ University of Stellenbosch, 2019. *Post Graduate Programmes in Information and Knowledge Management* [Online].

⁴⁹⁴ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁴⁹⁵ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁴⁹⁶ Jennex & Olfman, 2005. *Assessing Knowledge Management Success* p 33-49.

⁴⁹⁷ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 395.

⁴⁹⁸ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁴⁹⁹ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 396.

⁵⁰⁰ Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4021.

⁵⁰¹ Manhart & Thalmann, 2015. *Protecting Organizational Knowledge: A Structured Literature Review* p 204.

⁵⁰² Cheung *et al.*, 2012. *Development of an Organizational Knowledge Capabilities Assessment (OKCA) Method for Innovative Technology Enterprises* p 54-65.

⁵⁰³ Ahmad *et al.*, 2014. *Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective* p 27-39.

causing reputational damage; and ultimately a loss of revenue and productivity. Additionally, Mills and Smith⁵⁰⁴ found knowledge protection to be a statistically significant factor in organisational performance, further emphasising its importance.

While these concerns are relevant, the focus on sharing is not unjustified, nor should it be ignored. Donnelly⁵⁰⁵ argues that knowledge sharing is critical to ensuring organisational success and competitive advantage. However, only focusing on sharing creates an imbalance, in terms of attending to other CSFs, which ironically could lead to less effective knowledge sharing in turn⁵⁰⁶. Ilvonen *et al.* argue that it would rather make sense to focus on knowledge security in conjunction with knowledge sharing⁵⁰⁷, as they should be viewed as complimentary activities⁵⁰⁸, rather than as factors in opposition with one another. In terms of this balance, knowledge security can play a critical role in ensuring that knowledge sharing is more targeted by eliminating overload⁵⁰⁹. Although this balance is complex and sometimes controversial⁵¹⁰, accounting for both factors can result in more efficient security and KM processes.

In conclusion, it appears that leveraging knowledge security as a sustainable CSF would allow an organisation to ensure the ability of its KM activities and KMSs to continue to generate value and advantage for the organisation. Both in terms of protecting the critical knowledge that others may want and in terms of utilising the organisation's knowledge resources more efficiently. Achieving this is done through the effective use of knowledge security mechanisms, especially if those mechanisms can contribute to enhancing organisational performance as a result. Given that organisations rely on knowledge for their innovation capabilities and competitive success⁵¹¹, not focusing on knowledge security would seem to be detrimental, particularly when considering the benefits that have been outlined of integrating knowledge security with KM.

⁵⁰⁴ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 164.

⁵⁰⁵ Donnelly, 2019. *Aligning Knowledge Sharing Interventions with the Promotion of Firm Success: The Need for SHRM to Balance Tensions and Challenges* p 344.

⁵⁰⁶ Manhart & Thalmann, 2015. *Protecting Organizational Knowledge: A Structured Literature Review* p 190-191.

⁵⁰⁷ Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4021.

⁵⁰⁸ Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4021.

⁵⁰⁹ Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4021.

⁵¹⁰ Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4021.

⁵¹¹ Lafuente *et al.*, 2019. *Determinants of Innovation Performance Exploring the Role of Organisational Learning Capability in Knowledge-Intensive Business Services (KIBS) Firms* p 42.

This is an important issue, when contextualised within the highly globalised nature of today's business environment, the growth in connectivity and the increase in threats towards an organisation's information and knowledge⁵¹². Thus, if an organisation is concerned with deriving the most value and advantage from its knowledge resources, it would make sense to give adequate attention to elements such as knowledge security too, since not doing so can lead to a reduction in an organisation's ability to use knowledge to derive value and advantage. All of which may result in the organisation risking its ability to remain innovative in a highly competitive, globalised marketplace.

4.4 Identifying Knowledge Security Paradigms

As outlined in Chapter 1, when thinking about defining KM, particularly in terms of its applicability to organisations, most KM authors do not consider security in their approaches to managing knowledge⁵¹³. While some authors have aimed to rectify this oversight, it is not always clear if their proposed solutions are broad enough to deal with the complexities of securing knowledge in organisations. Further, as Manhart and Thalmann highlight, this lack of clarity and scope also corresponds to a lack of research focus on knowledge security, causing it to be underdeveloped⁵¹⁴. From a knowledge security perspective, this is observed by the lack of a unified KM framework through which to overlay and apply knowledge security systematically, resulting in increased fragmentation.

With this context in mind, to add clarity, I reviewed and analysed the literature through a process of categorisation and synthesis⁵¹⁵. I did this to consolidate the various approaches to knowledge security into relevant paradigms and to determine the subsequent perspectives for each paradigm. The analysis was framed from the perspective of how knowledge security is perceived and discussed in the literature, determined by the focus area of the texts evaluated. In terms of my methodological approach to reviewing the literature, my structure was based upon components of the literature review process outlined by Manhart and Thalmann⁵¹⁶. I adapted this from their published literature review of the knowledge protection literature⁵¹⁷.

⁵¹² Costa et al., 2019. *The Security Challenges Emerging from the Technological Developments: A Practical Case Study of Organizational Awareness to the Security Risks* p 1-6.

⁵¹³ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 86.

⁵¹⁴ Manhart & Thalmann, 2015. *Protecting Organizational Knowledge: A Structured Literature Review* p 190.

⁵¹⁵ Russell, 2005. *An Overview of the Integrative Research Review* p 2.

⁵¹⁶ Manhart & Thalmann, 2015. *Protecting Organizational Knowledge: A Structured Literature Review* p 193.

⁵¹⁷ Manhart & Thalmann, 2015. *Protecting Organizational Knowledge: A Structured Literature Review* p 193.

The decision to use components of their structure was premised on the usefulness of their framework as a starting point to identify and categorise the literature. However, it should be noted that due to the difference in our objectives, not all aspects of their process were deemed to be relevant. Manhart and Thalmann's process follows three stages, namely: 1) The identification of the literature. 2) Structuring the review. 3) Theoretical development. Each of these components can be broken down further into a series of sub-steps⁵¹⁸, as shown in Figure 4-3.

Figure 4-3: Manhart and Thalmann's Literature Review Process



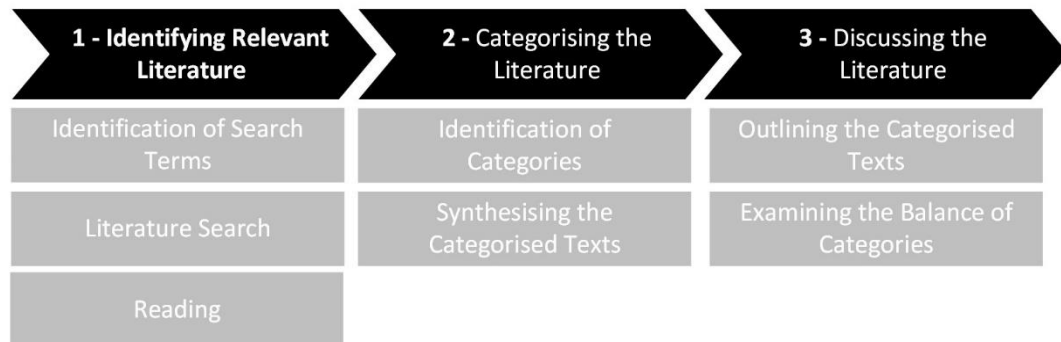
For Manhart and Thalmann⁵¹⁹, the purpose of their review was to firstly identify areas for further research, and secondly, to establish a research agenda based around the textual relationships identified in their concept matrix. Differing from this, my objective was to first categorise the paradigms and perspectives within the literature, and second, to understand the concepts and associated approaches to knowledge security. Of the components and sub-steps outlined by Manhart and Thalmann, Step 1 was deemed to be the most relevant due to its agnostic nature. By this, I mean that for either of our objectives it would be a useful framework to follow; structurally but not necessarily methodologically. For Steps 2 and 3, as our research objectives differed, the sub-steps were not deemed to be as relevant. For Step 2, my objective was to categorise the literature and synthesise it according to the paradigmatic focus of the texts. For Step 3, I aimed to outline and discuss the categorised texts and balance of the paradigms. Thus, unlike Manhart and Thalmann, I did not need to use qualitative analysis software, such as ATLAS.ti, to analyse the texts for complex phenomena hidden in

⁵¹⁸ Manhart & Thalmann, 2015. *Protecting Organizational Knowledge: A Structured Literature Review* p 193.

⁵¹⁹ Manhart & Thalmann, 2015. *Protecting organizational knowledge: a structured literature review* p 190.

unstructured data⁵²⁰. The steps discussed here will be expanded upon in the sections to follow, with my adapted review and categorisation process being outlined in Figure 4-4.

Figure 4-4: Adapted Literature Review, Categorisation and Discussion



4.4.1 Step 1 – Identifying Relevant Literature

The objective of Step 1 was to identify relevant knowledge security literature. I did this to gain an overview of the literature and to help eliminate texts not deemed to be relevant to my research objectives. Each of the sub-steps of Step 1 will now be discussed in more detail in the sections to follow.

4.3.1.1 Identification of Search Terms

Beginning with the first sub-step, a term harvesting⁵²¹ approach was used in line with general term harvesting techniques⁵²². I did this to establish an initial list of search terms and to refine them as the search process progressed. As the process was handled iteratively, although discussed separately here, sub-steps were sometimes conducted in parallel. I did this due to the nature of the process and its requirement for feedback in identifying new terms.

Acting as an anchor point, the term ‘knowledge security’ was used as the primary search term in the initial phase of the research. It is the main term associated with the broader research objectives of this dissertation and was used during the proposal phase. Using the term ‘knowledge security’ to conduct broad searches in Google Scholar and various journal databases⁵²³, additional terms were harvested. The additional terms were identified as they appeared in the search results and as they were found in the subsequently identified texts. When

⁵²⁰ Lewins *et al.*, 2007. *Using Software in Qualitative Research: A Step-by-Step Guide* p 17-32.

⁵²¹ Riesenber, 2014. *Conducting a Successful Systemic Review of the Literature, Part 1* p 16.

⁵²² University of Pennsylvania Libraries, 2019. *Systemic Reviews: Literature Search* [Online].]

⁵²³ Examples of databases included were Ebsco, Jstor, Sciverse, ProQuest, Emerald and more.

extracting terms from the texts, common or similar terms that appeared in the texts which referenced the protection of knowledge were harvested. In addition, terms were also harvested from other sources that the articles referenced in their bibliographies. I did this to identify a broad enough subset of terms covering an adequate breadth of the published material when searching.

The outcome of this process resulted in a list of core search terms found, and used for database searches, as follows:

- Knowledge security,
- Secure knowledge management,
- Securing knowledge,
- Knowledge management espionage,
- Secure knowledge sharing,
- Knowledge management and security,
- Information security and knowledge management,
- Knowledge protection,
- Knowledge risk management,
- Knowledge management and risk management,
- Risk management and knowledge and
- Intellectual capital protection.

4.3.1.2 Literature Search

Proceeding with the second sub-step, these terms were then used to conduct searches to identify relevant literature. This was done in the form of a digital literature search based on the use of Google Scholar. Google Scholar was used as an initial search base to broadly identify relevant authors and texts. Following the identification of these initial results, a deeper analysis was done by searching through academic journal databases, using the Stellenbosch University Library system's integrated search portal. The portal search covered an array of journal articles, books, e-theses, dissertations, digital collections, databases, reports and conference proceedings. The purpose of this deeper analysis was to ensure that all articles that were possibly accessible, some of which were locked behind pay walls on Google Scholar results, were covered. It was also done to focus on certain areas of interest, beyond the realms of the

general material presented in Google Scholar's search results. Through this search process, I identified 78 preliminary articles.

4.3.1.3 Reading

Proceeding with the third sub-step, I read through each of the article's abstracts, introductions, and summaries. In the case of longer texts, I also looked through their indexes for sections deemed to be relevant. This approach was followed to gauge the text's relevance to my research objectives and to eliminate non-relevant texts. Concerning this process, articles were eliminated for two reasons. Firstly, if they were incorrectly identified and were thus deemed to be completely irrelevant to my research objectives. Secondly, that some articles focused on security and KM, but from the perspective of using KM as a mechanism to help manage information security knowledge or similar. Having finished the reading and elimination process, I was left with 38 texts that were still deemed to be relevant to my research objectives. Thus, I began the process of reading through each of them in detail. The purpose of this is to extrapolate further search terms, authors or bibliographic references which could be used to search for more material. As part of this process, alternative terms relevant to knowledge security were highlighted for categorisation. In addition, key sections were also highlighted, and notes were made accordingly for further analysis.

4.4.2 Step 2 – Categorising the Literature

The objective of Step 2 was to categorise the identified literature in preparation for synthesising the results of the categorisations. I did this to structure the identified literature into common paradigms and views, in an integrated way⁵²⁴, for the eventual purpose of outlining the categorisations. In the sub-section to follow, I will discuss how the literature was categorised, followed by an overview of the categories used as relating to paradigms and perspectives.

4.3.2.1 Identification of Categories

Beginning with the first sub-step, a literature evaluation approach was used based on the principles of observation⁵²⁵ and analysis⁵²⁶. This approach was chosen as it was deemed the best fit for constructing the framework needed, upon which to provide a deeper category-based

⁵²⁴ Russell, 2005. *An Overview of the Integrative Research Review* p 1-2.

⁵²⁵ Goddard & Melville, 2004. *Research Methodology: An Introduction*.

⁵²⁶ Bernard, 2011. *Research Methods in Anthropology* p 7.

comparison. Given points out that categorisation, through observation in the form of deduction and/or induction⁵²⁷, is an important step in allowing researchers the opportunity to make meaning out of information that has been collected. It is also a major component of qualitative data analysis⁵²⁸. Given states that the objective of this approach is to derive “similarities of meaning between the individually coded bits as observed by the researcher”⁵²⁹. Given explains that this helps to discern semantic, logical, or theoretical links and connections between the different categories when abstracted or conceptualised further⁵³⁰. It is also a useful approach to use when creating themes, constructs or domains based on the analytical process of examining patterns across the categories⁵³¹.

When constructing a system of categories, as Given highlights, it is important to continue the categorisation process until saturation has been achieved⁵³². Saturation in this instance is defined as making sure the “existing system of categories accounts for all meaningful or significant aspects of the phenomenon in question”⁵³³. In this regard, it is also important that the process is completed to validate the internal integrity of each category, based on the level of homogeneity, as well as external integrity, based on the level of heterogeneity between categories⁵³⁴. The objective of which being that researchers should create a comprehensive system of categories so no meaningful area of the analysis falls outside of the array of categories.

Thus, categorising the literature into paradigms and perspectives was done to illuminate the most common focus areas and approaches used when engaging with knowledge security. By doing so, I was able to identify how the texts framed the importance of knowledge security in terms of what aspects of KM they focused on. This allowed me to determine the scope of the application when dealing with the concept of knowledge security, both in terms of the research focus and the possible practical implementation. Regarding the process of categorising themes, it consisted of the initial identification of paradigms and perspectives based on the focus area

⁵²⁷ Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

⁵²⁸ Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

⁵²⁹ Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

⁵³⁰ Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

⁵³¹ Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

⁵³² Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

⁵³³ Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

⁵³⁴ Given (Ed.), 2008. *Categorization In: The SAGE Encyclopaedia of Qualitative Research Methods* p 73.

of the texts. For example, if after reading a text it was deemed that the paradigmatic focus area of the text was the application of security mechanisms to a KMS, it would be categorised as a ‘System Security Paradigm’. Should the same text frame its discussion from a modelling and algorithmic view, the text would be categorised as a ‘Model and Algorithmic Perspective’ within the ‘System Security Paradigm’ and so on. The paradigms and perspectives were then listed with a reference code being given to both the listed paradigm, perspective, and matching text. The paradigms, perspectives and texts were then checked again and refined further, as needed, to ensure correctness.

In terms of the categories identified, these were: DIS Paradigm; Systems Security Paradigm; Assurance Paradigm; and a Risk Management Paradigm. The ‘DIS Paradigm’ was assigned to texts that dealt with knowledge security from a DIS view. These are texts that are framed from the perspectives of either looking at how DIS security functions could be applied to knowledge security in organisations or the general application of knowledge security in the military context. The ‘Systems Security Paradigm’ was assigned to those texts that dealt with issues of knowledge security from a systems security perspective. These are texts that are focused on perspectives relating to technical security controls, algorithmic approaches for handling knowledge security, issues of espionage, and broader architecture and management considerations from a computer systems perspective. The ‘Assurance Paradigm’ was assigned to those texts that dealt with knowledge security from an assurance driven view. These are texts that are focused on non-technical security issues, structural management issues, examining security as a success factor for KM, and the integration and research mapping of information security approaches with KM. The ‘Risk Management Paradigm’ focused on those texts that dealt with knowledge security from a risk management view. These are texts that deal with issues related to the retention of employee knowledge, the need for balancing sharing and securing of knowledge, and the integrated knowledge risk perspective.

4.3.2.2 Synthesising the Categorised Texts

This sub-step was used to help set a structural framework to outline the categorised paradigms and perspectives found in the literature. From a methodological perspective, I achieved this by using a concept matrix-based synthesis approach⁵³⁵. Taking this approach helped to meet my objectives by setting the groundwork for the categorisation and outlining of the literature.

⁵³⁵ University of Nevada, 2019. *Writing and Speaking Center: How to Use a Concept Matrix* p 1-2.

Practically, this meant looking for commonalities when identifying the various paradigms and perspectives of the texts, as to how they view and frame knowledge security. This helped me to determine what aspects the texts focused on the most and what areas may have been neglected. It also allowed for a more relevant analysis of the motivation and applicability of knowledge security theory and how this might translate to practice from a conceptual view. From this synthesis process, the resultant categorisation-based concept matrix was developed, as shown in Table 4-5, which will be discussed in more detail in the section to follow.

4.4.3 Step 3 – Discussing the Literature

I began by outlining each of the categorised texts as per their paradigms and perspectives as summarised in Table 4-5. I did this to complete the literature review process by examining the various security approaches in the literature as they relate to KM. I followed with a brief discussion around the composition of the categories, relating to the core paradigms. This was framed from the perspective of ascertaining why certain paradigms have more of a research focus than others.

4.3.3.1 A DIS Paradigm Relating to Knowledge Security in Organisations

In line with the framework discussed above, concerning a ‘DIS Paradigm’, two key perspectives were identified from the literature within this general knowledge security categorisation. These are: 1) Applying DIS Knowledge Security Principles to Organisations. 2) General Analysis of KM and Security in the Military Context. These aspects are discussed in the paragraphs to follow.

Applying DIS Knowledge Security Principles to Organisations – Desouza and Vanapalli⁵³⁶ highlight the dynamic between the growth in importance of knowledge assets for organisations and the lack of established measures to protect them from a KM perspective. As this is not the case with the DIS sector, they propose that non-DIS organisations can use the DIS model as a template for better knowledge protection. This template follows three areas of focus consisting of people, products, and processes. Each of these areas also has corresponding sub-facets and will be briefly outlined further.

⁵³⁶ Desouza & Vanapalli, 2005. *Securing Knowledge in Organisations: Lessons from the Defence and Intelligence Sectors* p 85-87.

Table 4-5: Categorisation-Based Concept Matrix of Paradigms, Perspectives and Authors

Category	Author
A DIS Paradigm Relating to Knowledge Security in Organisations - Total: 2 texts	
Applying DIS Knowledge Security Principles to Organisational Perspective Count: 1 text	<ul style="list-style-type: none"> Desouza & Vanapalli, 2005. <i>Securing Knowledge in Organisations: Lessons from the Defence and Intelligence Sectors</i>
General Analysis of KM and Security in the Military Context Perspective Count: 1 text	<ul style="list-style-type: none"> Putter, 2018. <i>Knowledge Management for the South African Department of Defence</i>
A Systems Security Paradigm Relating to Knowledge Security in Organisations - Total: 18 texts	
A Technical Systems Perspective Count: 7 texts	<ul style="list-style-type: none"> Newswire, 2000. <i>Swiss Real Estate Group, Maag Holdings, Selects RSA Keon and RSA SecurID to Help Secure Knowledge Management System</i> Mundy and Chadwick, 2004. <i>Secure Knowledge Management for Health Care Organisations</i> Lee <i>et al.</i>, 2005. <i>Secure Knowledge Management and the Semantic Web</i> Ahmad & Ewe, 2005. <i>A Model for Secure Knowledge Sharing</i>. Upadhyaya, 2006. <i>Secure Knowledge Management</i> Thuraisingham and Parikh, 2008. <i>Trustworthy Semantic Web Technologies for Secure Knowledge Management</i> Ruiz <i>et al.</i>, 2011. <i>A Framework and Implementation for Secure Knowledge Management in Large Communities</i>
An Espionage and Counterespionage Perspective Count: 1 text	<ul style="list-style-type: none"> Lee & Rosenbaum, 2003. <i>Knowledge Management: Portal for Corporate Espionage? Defining the Problem Part 1</i>

Category	Author
<p>A Model and Algorithmic Perspective</p> <p>Count: 4 texts</p>	<ul style="list-style-type: none"> • Xu & Zhang, 2004. <i>PBKM: A Secure Knowledge Management Framework</i> • Malatras <i>et al.</i>, 2005. <i>Secure and Distributed Knowledge Management in Pervasive Environments</i> • Arora <i>et al.</i>, 2006. <i>Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis</i> • Boella & van der Torre, 2006. <i>Security Policies for Sharing Knowledge in Virtual Communities</i>
<p>An Architecture and Management Perspective</p> <p>Count: 6 texts</p>	<ul style="list-style-type: none"> • Randeree, 2006. <i>Knowledge Management: Securing the Future</i> • Muniraman <i>et al.</i>, 2007. <i>Security and Privacy Issues in a Knowledge Management System</i> • Memon & Daniels, 2007. <i>Special Issue on Secure Knowledge Management</i> • Hota <i>et al.</i>, 2015. <i>Advances in Secure Knowledge Management in the Big Data Era</i> • Singh & Salam, 2006. <i>Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective</i> • Bertino <i>et al.</i>, 2006. <i>Secure Knowledge Management: Confidentiality, Trust, and Privacy</i>
An Assurance Paradigm Relating to Knowledge Security in Organisations - Total: 11 texts	
<p>A Non-Technical Security Measures Perspective</p> <p>Count: 4 texts</p>	<ul style="list-style-type: none"> • Desouza, 2006. <i>Knowledge Security: An Interesting Research Space</i> • Desouza, 2007. <i>Managing Knowledge Security: Strategies for Protecting your Company's Intellectual Assets</i> • Popescul, 2011. <i>The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation</i> • Ilvonen <i>et al.</i>, 2016. <i>Knowledge Sharing and Knowledge Security in Finnish Companies</i>

Category	Author
A Structural Management Perspective Count: 2 texts	<ul style="list-style-type: none"> Ryan, 2006. <i>Political Engineering in Knowledge Security</i> Harris <i>et al.</i>, 2007. <i>Standards for Secure Data Sharing Across Organisations</i>
A Security and Success Factor Perspective Count: 4 texts	<ul style="list-style-type: none"> Holsapple & Joshi, 2000. <i>An Investigation of Factors that Influence the Management of Knowledge in Organisations</i> Park, 2006. <i>Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study</i> Jennex & Zyngier, 2007. <i>Security as a Contributor to Knowledge Management Success</i> Mills & Smith, 2011. <i>Knowledge Management and Organisational Performance: A Decomposed View</i>
An Integration and Research Mapping Perspective Count: 1 text	<ul style="list-style-type: none"> Jennex & Durcikova, 2014. <i>Integrating IS Security with Knowledge Management: Are we Doing Enough to Thwart the Persistent Threat?</i>
A Risk Management Paradigm Relating to Knowledge Security in Organisations - Total: 7 texts	
A Knowledge Retention Perspective Count: 3 texts	<ul style="list-style-type: none"> IAEA, 2006. <i>Risk Management of Knowledge Loss in Nuclear Industry Organisations</i> Boyles <i>et al.</i>, 2009. <i>Risk Management of Knowledge Loss in Nuclear Industry Organisations</i> Jennex, 2014. <i>A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel</i>
A Balanced Sharing Perspective Count: 1 text	<ul style="list-style-type: none"> Ryan, 2006. <i>Managing Knowledge Security</i>
An Integrated Knowledge Risk Perspective Count: 3 texts	<ul style="list-style-type: none"> Shedden <i>et al.</i>, 2011. <i>Incorporating a Knowledge Perspective into Security Risk Assessments</i> Padyab, 2014. <i>Genre-Based Approach to Assessing Information and Knowledge Security Risks</i> Thalmann <i>et al.</i>, 2014. <i>An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection</i>

Firstly, from a people-driven perspective, Desouza and Vanapalli⁵³⁷ outline the sub-facets as training and indoctrination, security clearances, and counterintelligence. They explain that the objective of training and indoctrination is to instil within new employees a code of conduct, using a knowledge-sharing approach, to generate competency and foster allegiance to the organisation. As they explain, security clearances are focused on ensuring that only authorised individuals have access to relevant knowledge⁵³⁸. Clearance is managed through access applications, background checks and interviews to determine competency. Counterintelligence, operating independently of other functions, monitors employee activities to ensure that classified knowledge is used appropriately. The value lies in the ability of counterintelligence to mitigate risk, either by pre-empting a threat or by intervening after an incident has occurred.

Secondly, from a product-driven perspective, Desouza and Vanapalli⁵³⁹ outline the sub-facets as documenting, tagging documents, securing devices, and segmenting documents. Documenting focuses on processes, activities and repositories used to capture an organisation's explicit knowledge in a highly structured and standardised way. Tagging documents focuses on tracking the history and connectivity of documents through an archival database to ensure they cannot be deleted without authorisation, are destroyed properly, and no security breaches have occurred. Securing devices means tagging digital devices with radio frequency identification (RFID) tags to monitor their location and status. The purpose is to ensure they are not removed from the organisation, or unauthorised devices brought in. Segmenting documents involves sorting them according to security clearance levels and marking them appropriately. The objective is to do this in a balanced way, regarding securing and sharing, to identify the most sensitive knowledge. It also ensures that only those who have the right level of clearance can access specific documents.

Thirdly, from a process-driven perspective, Desouza and Vanapalli⁵⁴⁰ outline the sub-facets as security of the knowledge process, security of knowledge channels and leadership. Security of

⁵³⁷ Desouza & Vanapalli, 2005. *Securing Knowledge in Organisations: Lessons from the Defence and Intelligence Sectors* p 88-89.

⁵³⁸ Desouza & Vanapalli, 2005. *Securing Knowledge in Organisations: Lessons from the Defence and Intelligence Sectors* p 88-89.

⁵³⁹ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 90-93.

⁵⁴⁰ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 93-96.

the knowledge process focuses on the protection of knowledge generation and application processes from unauthorised disclosure, destruction, or modification. To achieve this, focus is given to identification, authentication, authorisation, and integrity. Security of knowledge channels ensures that only authorised knowledge is communicated over authorised channels and that backup communication channels are available. Leadership focuses on having support from senior organisational members and ensuring direction and foresight through “clear, frequent, and open communication with their staff members on a regular basis”⁵⁴¹. The objective is to ensure that KM solutions are used and KM initiatives are not wasted.

General Analysis of KM and Security in the Military Context – Putter examines the application of KM to the South African Department of Defence, outlined from the perspective of intelligence⁵⁴², with knowledge security forming part of this approach. Knowledge security in this sense should cover both explicit and tacit knowledge not yet imparted⁵⁴³ and ensure the protection and quality of knowledge resources⁵⁴⁴ from an effects and advantage standpoint⁵⁴⁵. As such, Putter discusses that knowledge has more depth than data or information and should be secured uniquely⁵⁴⁶, beyond standard security approaches⁵⁴⁷. Doing so should support the mission command principle of creating a shared understanding by securely connecting the right people⁵⁴⁸. Putter makes an additional observation related to knowledge protection needing to be a distinct KM process⁵⁴⁹ integrated with policy, information management and KM⁵⁵⁰. He outlines that this is currently not the case as it is viewed by some as an inhibitor to sharing and innovation⁵⁵¹ or that the protection of knowledge is already implicit in IT enablers and policy⁵⁵². If knowledge protection is not viewed as a distinct process, Putter argues that competitive

⁵⁴¹ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 93-96.

⁵⁴² Putter, 2018. *Knowledge Management for the South African Department of Defence* p 352.

⁵⁴³ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 42.

⁵⁴⁴ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 81.

⁵⁴⁵ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 96.

⁵⁴⁶ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 137.

⁵⁴⁷ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 137.

⁵⁴⁸ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 133.

⁵⁴⁹ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 75.

⁵⁵⁰ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 133.

⁵⁵¹ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 132.

⁵⁵² Putter, 2018. *Knowledge Management for the South African Department of Defence* p 75.

advantage might be lost due to the occurrence of knowledge vulnerabilities resulting from subsequent negligence or oversight⁵⁵³.

4.3.3.2 A Systems Security Paradigm Relating to Knowledge Security in Organisations

In line with the framework discussed above, concerning a ‘Systems Security Paradigm’, four key perspectives were identified from the literature within this general knowledge security categorisation. These are: 1) A Technical Systems Perspective. 2) An Espionage and Counterespionage Perspective. 3) A Model and Algorithmic Perspective. 4) An Architecture and Management Perspective. These are discussed in the paragraphs to follow.

Technical Systems Perspective – Most of the authors analysed in the ‘Systems Security Paradigm’ focused on the security of KMSs from a technical perspective, like a regular information system. Framing a KMS in this way allows for the application of information security and assurance measures to it, dealing with many of the same issues. For example, Newswire⁵⁵⁴ reported on the application of RSA technologies to ensure secure access control to a Swiss real estate group’s KMS. The approach outlined focused on using two-factor authentication and a public key interface system for access, as would be done with regular information systems. As it is a news article, the approach reported on is not in-depth and does not mention what other elements of the KMS might need to be secured.

Mundy and Chadwick⁵⁵⁵ also view KMSs in the same light, by framing their security from an information security and risk reduction view. Practically, this means the implementation of solutions like hashed passwords, biometrics, cryptography, access control systems, firewalls and security policies relating to storage, backups, and the secure disposal of knowledge assets⁵⁵⁶. Thus, they argue that secure KM is essential for securing a KMS when capturing, storing, distributing, using, destroying, and restoring knowledge.

Similarly, Lee *et al.* highlight the importance of protecting organisational knowledge⁵⁵⁷ by applying an IT-based systems security approach, built for the needs of a KMS, acting as part

⁵⁵³ Putter, 2018. *Knowledge Management for the South African Department of Defence* p 75.

⁵⁵⁴ Newswire, 2000. *Swiss Real Estate Group, Maag Holdings, Selects RSA Keon and RSA SecurID to Help Secure Knowledge Management System* p 1-3.

⁵⁵⁵ Mundy & Chadwick, 2005. *Secure Knowledge Management for Health Care Organisations* p 321-322.

⁵⁵⁶ Mundy & Chadwick, 2005. *Secure Knowledge Management for Health Care Organisations* p 323-329.

⁵⁵⁷ Lee *et al.*, 2005. *Secure Knowledge Management and the Semantic Web* p 50.

of the semantic web⁵⁵⁸. Lee *et al.* view this as vital and as they outline in addition to information systems, attention must also be paid to protecting strategic knowledge resources⁵⁵⁹. According to Lee *et al.*, if this is not done and critical knowledge is stolen, an organisation may lose its competitive advantage⁵⁶⁰. They then propose similar practical solutions as Mundy and Chadwick⁵⁶¹ but with a focus on Extensible Mark-up Language (XML) and Resource Description Framework (RDF)⁵⁶² related security issues⁵⁶³.

Ahmad and Ewe⁵⁶⁴ take an automated security approach related to preserving the authenticity and integrity of digital knowledge objects. They propose doing so by using a model centred on the CIA triad. The model they propose, the Secure Knowledge Acquisition and Retrieval (SKAR) model, aims to automate the detection and recovery mechanisms for tampered knowledge objects, to make sure that knowledge processing resources always continue to perform correct processing operations within the system⁵⁶⁵.

Upadhyaya *et al.*⁵⁶⁶, propose a secure content management framework highlighting the importance of security for an organisation's data, information, knowledge, and the applications used to retain them. Practically, this means implementing information security elements such as authentication control, passwords, cryptography, intrusion detection systems, access control systems, and security policies, the objective being to guard against insider threats and protect knowledge infrastructure through the refinement and enforcement of the framework.

Thuraisingham and Parikh take a layered semantic web technology view⁵⁶⁷ focused on protecting knowledge resources through automation⁵⁶⁸. As with Lee *et al.*, Thuraisingham and Parikh discuss security issues relating to XML and the RDF⁵⁶⁹. The security mechanisms they

⁵⁵⁸ Lee *et al.*, 2005. *Secure Knowledge Management and the Semantic Web* p 48.

⁵⁵⁹ Lee *et al.*, 2005. *Secure Knowledge Management and the Semantic Web* p 50.

⁵⁶⁰ Lee *et al.*, 2005. *Secure Knowledge Management and the Semantic Web* p 50.

⁵⁶¹ Mundy & Chadwick, 2005. *Secure Knowledge Management for Health Care Organisations* p 321-322.

⁵⁶² RDF is the standard semantic model for data interchange on the web.

⁵⁶³ Lee *et al.*, 2005. *Secure Knowledge Management and the Semantic Web* p 52-54.

⁵⁶⁴ Ahmad & Ewe, 2005. *A Model for Secure Knowledge Sharing* p 1-2.

⁵⁶⁵ Ahmad & Ewe, 2005. *A Model for Secure Knowledge Sharing* p 3-4.

⁵⁶⁶ Upadhyaya, 2006. *Secure Knowledge Management* p 1.

⁵⁶⁷ Thuraisingham & Parikh, 2008. *Trustworthy Semantic Web Technologies for Secure Knowledge Management* p 186-187.

⁵⁶⁸ Thuraisingham, 2004. *Secure Knowledge Management*.

⁵⁶⁹ Thuraisingham & Parikh, 2008. *Trustworthy Semantic Web Technologies for Secure Knowledge Management* p 186-187.

propose are centred on information security principles to secure the handling of customer information, supply chains, and digital documents⁵⁷⁰. Where they differ from Lee *et al.* is that they extend the scope of their framework to include broader KMS security issues. They do so by focusing on aspects like collaboration, access rights and the implications of e-business⁵⁷¹.

Ruiz *et al.*⁵⁷² discuss the security requirements concerning knowledge and systems from a broader ontological framework. They state that organisations need to provide KM tools that are convenient to use and help to share knowledge in an easily secured way⁵⁷³. As with Thuraisingham and Parikh⁵⁷⁴, they too highlight the importance of automation as an essential component of this process, based on systems security and privacy policies⁵⁷⁵. The approach here again⁵⁷⁶ is also on using and securing XML and RDF to achieve this purpose⁵⁷⁷.

Espionage and Counterespionage Perspective – In *Part 1* of their discussion on KM and security, Lee and Rosenbaum⁵⁷⁸ take a corporate espionage view of KM. They highlight that KM plays a critical role in gathering knowledge on competitors with KMSs being used to leverage this knowledge for competitive advantage. Yet, in doing so, a KMS is also a valuable target because of the richness of the knowledge it holds. If a competitor can gain access to an organisation's KMS, it will allow them to gain critical insight into the organisation's knowledge and business practices⁵⁷⁹. This can result in a competitor identifying where an organisation's knowledge gaps are and how they can be exploited for competitive gain.

⁵⁷⁰ Thuraisingham & Parikh, 2008. *Trustworthy Semantic Web Technologies for Secure Knowledge Management* p 189.

⁵⁷¹ Thuraisingham & Parikh, 2008. *Trustworthy Semantic Web Technologies for Secure Knowledge Management* p 189.

⁵⁷² Ruiz *et al.*, 2011. *A Framework and Implementation for Secure Knowledge Management in Large Communities* p 5.

⁵⁷³ Ruiz *et al.*, 2011. *A Framework and Implementation for Secure Knowledge Management in Large Communities* p 1.

⁵⁷⁴ Thuraisingham & Parikh, 2008. *Trustworthy Semantic Web Technologies for Secure Knowledge Management* p 189-193.

⁵⁷⁵ Ruiz *et al.*, 2011. *A Framework and Implementation for Secure Knowledge Management in Large Communities* p 1.

⁵⁷⁶ Lee *et al.*, 2005. *Secure Knowledge Management and the Semantic Web* p 52-54.

⁵⁷⁷ Ruiz *et al.*, 2011. *A Framework and Implementation for Secure Knowledge Management in Large Communities* p 6-8.

⁵⁷⁸ Lee & Rosenbaum, 2003. *Knowledge Management: Portal for Corporate Espionage? Defining the Problem Part 1* p 14.

⁵⁷⁹ Lee & Rosenbaum, 2003. *Knowledge Management: Portal for Corporate Espionage? Defining the Problem Part 1* p 16.

In *Part 2* of their discussion, Lee and Rosenbaum⁵⁸⁰ pay attention to the security mechanisms needed to counter the technical and insider threats targeting KMSs. The controls that they suggest are access rights and the monitoring of insider activities. They argue that taking this approach helps to balance the needs of restricting and sharing access to KMSs, which should be revisited and adjusted over time. Thus, they recommend that for effective security to take place, there needs to be a collaboration between the IT security and KM functions of an organisation, in developing and securing KM initiatives and systems.

Model and Algorithmic Perspective – Xu and Zhang⁵⁸¹ discuss using a conceptual role-based framework for secure KM. They call this the ‘Privacy-preserving and Breaching-aware Knowledge Management’ (PBKM) framework⁵⁸². The PBKM is built around the extraction, sharing and utilisation of knowledge for collective problem-solving⁵⁸³. Their approach, when applied to a KMS, focuses on the alignment of KM procedures and processes through access control and privacy preservation⁵⁸⁴. These are framed as automated systems rules that govern the controls used to manage how knowledge is accessed and shared through the KMS. Practically, this involves using automation to determine breaches, focused on algorithmic pattern matching, and to ensure privacy by applying cryptographic rule sets to better manage service-based requests⁵⁸⁵.

Malatras *et al.*⁵⁸⁶ discuss the issue of security relating to distributed KM applications in pervasive environments. They take a systems-based approach by proposing a KMS architecture to enable KM operations to function robustly and securely⁵⁸⁷. Like the conceptual approach put forward by Xu and Zhang, Malatras *et al.*⁵⁸⁸ focus on the use of automation to secure KMSs. To ensure security and control, they discuss how an algorithmic approach can be used to manage the rules and actions of users in a KMS. Practically, they suggest using various security

⁵⁸⁰ Lee & Rosenbaum, 2004. *Knowledge Management: Portal for Corporate Espionage? Defining the Problem Part 2: Who Spies? How Can Enterprises be Knowledge Enabled yet Knowledge Secure?* p 10-11.

⁵⁸¹ Xu & Zhang, 2004. *PBKM: A Secure Knowledge Management Framework* p 2-6.

⁵⁸² Xu & Zhang, 2004. *PBKM: A Secure Knowledge Management Framework* p 2.

⁵⁸³ Xu & Zhang, 2004. *PBKM: A Secure Knowledge Management Framework* p 1.

⁵⁸⁴ Xu & Zhang, 2004. *PBKM: A Secure Knowledge Management Framework* p 1-6.

⁵⁸⁵ Xu & Zhang, 2004. *PBKM: A Secure Knowledge Management Framework* p 5-9.

⁵⁸⁶ Malatras *et al.*, 2005. *Secure and Distributed Knowledge Management in Pervasive Environments* p 79-83.

⁵⁸⁷ Malatras *et al.*, 2005. *Secure and Distributed Knowledge Management in Pervasive Environments* p 80.

⁵⁸⁸ Malatras *et al.*, 2005. *Secure and Distributed Knowledge Management in Pervasive Environments* p 83.

models for system governance and ensuring security mechanisms are designed into a KMS from the beginning.

Similarly, Arora *et al.*⁵⁸⁹ propose an autonomic-computing system approach to managing the security requirements of a KMS. This is focused on using high-level system objectives as the basis for managing KMS security. Practically, they suggest using algorithms to model the required security behaviour and system configuration options⁵⁹⁰, manifested as self-configuring, optimising, protecting, and healing elements⁵⁹¹. Arora *et al.*⁵⁹² argue that doing so creates a cyber technical focus for the application of security that can automatically respond with deterrence mechanisms if malicious traffic is detected, or to implement healing procedures needed if damage has been caused.

Boella and van der Torre⁵⁹³ propose the use of a security-driven, game-theoretic model to secure KMSs. As with the previous authors, the focus is on autonomic access control using algorithmic procedures⁵⁹⁴. They argue that this approach should be followed to respect the autonomy of knowledge providers and to meet the security requirements of a KMS when framed as a normative multiagent system⁵⁹⁵. Their approach differs from those proposed by Arora *et al.*, Malatras *et al.*, and Xu and Zhang, in that they focus heavily on system policies as the central driving force in managing the technical security requirements of the KMS; from both a high-level and granular perspective.

Architecture and Management Perspective – Randeree⁵⁹⁶ explains that a more inclusive approach is needed to manage KMS security requirements due to the difficulties associated with the contextual requirements of the knowledge types, infrastructure, and process architecture. Randeree outlines that at a minimum KMSs should have the same level of security

⁵⁸⁹ Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 487.

⁵⁹⁰ Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 489-495.

⁵⁹¹ Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 488.

⁵⁹² Arora *et al.*, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 488.

⁵⁹³ Boella & van der Torre, 2006. *Security Policies for Sharing Knowledge in Virtual Communities* p 5.

⁵⁹⁴ Boella & van der Torre, 2006. *Security Policies for Sharing Knowledge in Virtual Communities* p 6-10.

⁵⁹⁵ Boella & van der Torre, 2006. *Security Policies for Sharing Knowledge in Virtual Communities* p 1.

⁵⁹⁶ Randeree, 2006. *Knowledge Management: Securing the Future* p 148.

as an information system⁵⁹⁷, but optimally a more inclusive focus is needed⁵⁹⁸. The optimal focus is based on six core measurements. These are relationship capital (trust and partnerships); asset protection (protecting core know-how); knowledge environment (learning focus); knowledge transfer (capturing ability); ambiguity (competency and transferability); and tacitness (perceived level)⁵⁹⁹.

Muniraman *et al.*⁶⁰⁰ also discuss a more inclusive approach to securing KMSs based on information security and assurance mechanisms. They outline that the aspects that make up a KMS need to be viewed from a high-level perspective. They argue that this is important, as often KMSs are not thought of as critical systems and are then not afforded the same level of security as other IT systems. Further, they discuss that security mechanisms applied to KMSs need to be extended as the risks posed are unique⁶⁰¹. These risks result from the broad level of user access required of a KMS and the need to share knowledge on a large scale. Practically, this means focusing on the security issues that arise when having to add, update, share and provide knowledge to KMS users.

Memon and Daniels⁶⁰² outline the importance of the role played by knowledge processes and tools within the broader business and management context concerning KMSs. They argue that security issues can arise due to the dynamics of having to provide open and restricted access to knowledge, depending on the user and context. Following this introduction, the rest of the paper outlines the abstracts from key papers, reflecting this perspective, that were presented at the *Second Secure Knowledge Management Workshop*⁶⁰³.

Hota *et al.*⁶⁰⁴ discuss the need for a high-level view on managing and securing KMSs in the big data era. They explain that this is important due to the richness that using knowledge can afford, over information or data, in answering *how* questions and the associated increase in complexity⁶⁰⁵. Complexity in this instance arises as, in addition to traditional KM cycle inputs,

⁵⁹⁷ Randeree, 2006. *Knowledge Management: Securing the Future* p 145.

⁵⁹⁸ Randeree, 2006. *Knowledge Management: Securing the Future* p 149.

⁵⁹⁹ Randeree, 2006. *Knowledge Management: Securing the Future* p 149.

⁶⁰⁰ Muniraman *et al.*, 2007. *Security and Privacy Issues in a Knowledge Management System* p 45-2-10.

⁶⁰¹ Muniraman *et al.*, 2007. *Security and Privacy Issues in a Knowledge Management System* p 45-1.

⁶⁰² Memon & Daniels, 2007. *Special Issue on Secure Knowledge Management* p 449.

⁶⁰³ Memon & Daniels, 2007. *Special Issue on Secure Knowledge Management* p 449.

⁶⁰⁴ Hota *et al.*, 2015. *Advances in Secure Knowledge Management in the Big Data Era* p 983.

⁶⁰⁵ Hota *et al.*, 2015. *Advances in Secure Knowledge Management in the Big Data Era* p 984.

big data creates the need to include non-traditional inputs too, thus increasing the richness of knowledge captured in the system. Hota *et al.* argue that this creates the need for knowledge specific security requirements since organisations operate in an increasingly interconnected world, where the potential risk and threat profile facing KMSs has increased.

Singh and Salam⁶⁰⁶ discuss using a semantic information assurance-based framework to secure distributed KM elements. The system's objective is to handle reasoning, ontologies, and ways to discover common meaning for entity representations. To do this, they propose taking a holistic view by integrating three streams of research focused on e-business processes, information assurance, and semantic technology. Thus, their framework is primarily based on the use of semantic technology, with a focus on knowledge representation, structured collections and inference rules linked into a single automated system⁶⁰⁷. As they outline, knowledge codification, storage, retrieval, and sharing do not transpire in a vacuum. Rather, they occur through interaction in the context of business processes, be that in scientific, governmental, or commercial settings⁶⁰⁸. In the context of a business process, integrating a defined security approach provides the framework on which to develop a secure KM architecture. According to Singh and Salam⁶⁰⁹, this is particularly relevant where the focus is on managing explicit knowledge that is declarative enough to be represented by standards-based representation languages. Singh and Salam state that practically this involves “defining the roles, permissions, access, and security of resources of information and knowledge from a dynamic business process perspective”⁶¹⁰. As the authors explain, besides internal system security, combining this with both product, service and process knowledge allows for systems to be built for secure distributed KM across different business partner organisations.

⁶⁰⁶ Singh & Salam, 2006. *Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective* p 472.

⁶⁰⁷ Singh & Salam, 2006. *Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective* p 476.

⁶⁰⁸ Singh & Salam, 2006. *Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective* p 472.

⁶⁰⁹ Singh & Salam, 2006. *Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective* p 474.

⁶¹⁰ Singh & Salam, 2006. *Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective* p 474.

Bertino *et al.*⁶¹¹ argue that security needs to be integrated into the KM lifecycle for it to be effective⁶¹² and aligned with the KM and business strategies of the organisation. In line with the KM lifecycle⁶¹³, their approach centres on utilising the principles of confidentiality, trust, and privacy⁶¹⁴. Practically, this means following a rule-based systems approach structured around access control techniques, trust management and privacy controls hinging on key secure KM aspects and architecture. From a systems perspective, this means the application of role-based access control and usage control, credential mechanisms, and encryption⁶¹⁵. It also includes the application of trust management and negotiation frameworks. Bertino *et al.*⁶¹⁶ highlight that these are important, as KM often involves collaboration across multiple departments or organisations, and therefore requires adequate rules for managing collaboration. Issues of privacy are also important for secure KM to consider and can be managed through the application of technologies such as privacy-preserving data mining⁶¹⁷.

4.3.3.3 An Assurance Paradigm Relating to Knowledge Security in Organisations

In line with the framework discussed above, concerning an ‘Assurance Paradigm’, four key perspectives were identified from the literature within this general knowledge security categorisation. These are: 1) A Non-Technical Security Measures Perspective. 2) A Structural Management Perspective. 3) A Security and Success Factor Perspective. 4) An Integration and Research Mapping Perspective. These are discussed in the paragraphs to follow.

Non-Technical Security Measures Perspective – Desouza⁶¹⁸ builds upon his previous research as a foundation and outlines that the reason for executives wanting to find mechanisms to protect knowledge assets is twofold. Firstly, knowledge assets have value and hold a special salience for organisations as they provide an advantage, drive, use resources and are not easily substituted⁶¹⁹. Secondly, information security falls short as a sole knowledge protection mechanism, as knowledge assets are not easily visualised, are not products and are in a

⁶¹¹ Bertino *et al.*, 2006. *Secure Knowledge Management: Confidentiality, Trust, and Privacy* p 429.

⁶¹² Bertino *et al.*, 2006. *Secure Knowledge Management: Confidentiality, Trust, and Privacy* p 436.

⁶¹³ Bertino *et al.*, 2006. *Secure Knowledge Management: Confidentiality, Trust, and Privacy* p 436.

⁶¹⁴ Bertino *et al.*, 2006. *Secure Knowledge Management: Confidentiality, Trust, and Privacy* p 429.

⁶¹⁵ Bertino *et al.*, 2006. *Secure Knowledge Management: Confidentiality, Trust, and Privacy* p 429.

⁶¹⁶ Bertino *et al.*, 2006. *Secure Knowledge Management: Confidentiality, Trust, and Privacy* p 436.

⁶¹⁷ Bertino *et al.*, 2006. *Secure Knowledge Management: Confidentiality, Trust, and Privacy* p 430.

⁶¹⁸ Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 2.

⁶¹⁹ Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 2-4.

continuous state of flux; making them difficult to protect. Desouza⁶²⁰ argues that this creates a security misalignment, as organisations relegate security efforts to having technical mechanisms in place to ensure the security of their information systems. They then apply basic protocols such as identity badges for their human assets. In Desouza's opinion⁶²¹, these mechanisms and protocols do little to secure critical knowledge assets, as most knowledge security breaches exploit the non-technical weaknesses of an organisation⁶²².

Next, building on this research, Desouza argues that from a KM perspective, three barriers hinder organisations from effectively protecting their intellectual assets. These being that some organisations are still grappling with establishing an effective KM program; view security as a risk to sharing, or do not have a clear understanding of what needs to be protected⁶²³. To overcome these challenges, Desouza explores protecting intellectual assets from a more holistic perspective. He highlights that it is important to protect knowledge, which is used by the organisation to create value, as not all knowledge can or should be protected⁶²⁴. To protect intellectual assets, Desouza focuses on issues related to employees, ICT, alliances, physical security and crisis and disaster management.

As employees are holders of value, knowledge is at risk of compromise through their intentional or unintentional actions⁶²⁵. Compromise can occur from sloppiness, obsolescence, competition for talent, entrapment of an employee, or malicious intent⁶²⁶. To mitigate these risks, mechanisms like background checks, regular check-ups, counterintelligence, incentives, education, and aligning security objectives with organisational goals can be used⁶²⁷. Relating to ICT security issues, Desouza focuses on the human aspects of security when using

⁶²⁰ Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 6.

⁶²¹ Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 6.

⁶²² Desouza, 2006. *Knowledge Security: An Interesting Research Space* p 6.

⁶²³ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 11.

⁶²⁴ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 11.

⁶²⁵ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 22-23.

⁶²⁶ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 30.

⁶²⁷ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 30.

technology to carry out business activities⁶²⁸. Compromise can occur from theft of mobile devices, their external usage, sensitive discussions in public and using insecure communication channels⁶²⁹. To mitigate these risks, measures should be implemented to secure travellers and their electronic channels, and to prevent technology-enabled duplication, storage and application⁶³⁰. Concerning strategic alliance security issues, Desouza explains that when collaborating with an external entity, an organisation opens some aspect of its business to them. For example, when entering into licensing agreements, product, or development contracts or through joint ventures⁶³¹. Compromise can occur where the partner has weak security⁶³², sub-par performance, acting with guile, leaks, moving intellectual assets, hijacking and the incapacitation of the alliance⁶³³. These risks can be mitigated by ensuring an alliance of trust, monitoring behaviours and performance, incentives, and balancing risks⁶³⁴. Physical security issues pose a challenge to organisations that have large offices and a global footprint. Desouza discusses the importance of securing sensitive knowledge in premises and ensuring that facilities used for offsite meetings are secured. Additionally, he discusses the importance of protecting executives who travel⁶³⁵. Compromise can occur from intruders, foreign objects, offsite facilities, eavesdropping, how assets are handled when removed, assaults and high-risk neighbours. To mitigate these risks, measures should be implemented to control access points, monitor guests, inspections, working with neighbours and handle security on the go⁶³⁶. Crises and disasters can arise from both natural and human events. Here an organisation needs to prepare measures not only to protect knowledge loss but also to plan for the resumption of operations. Compromise can occur if the organisation is abnormally reactive and does not think

⁶²⁸ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 58.

⁶²⁹ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 58.

⁶³⁰ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 59.

⁶³¹ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 22-23.

⁶³² Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 23-24.

⁶³³ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 23-24.

⁶³⁴ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 23-24.

⁶³⁵ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 24.

⁶³⁶ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 107.

through the consequence of its actions⁶³⁷. To mitigate these risks, organisations should think through, plan, rehearse and be ready for these situations before they materialise⁶³⁸.

Finally, Desouza ties this together by discussing how to assimilate these lessons through the implementation of several strategic considerations⁶³⁹. These include building a team; public relations; evaluation and monitoring of the security function; building or outsourcing it, local or global security; and prioritising goals and objectives. The objective of this approach is to support an understanding of an organisation's knowledge security landscape. Practically, this means focusing on preventative measures such as contingency plans, scenarios, immediate response capabilities, learning capabilities and having virtual monitoring stations in place⁶⁴⁰.

Popescul⁶⁴¹ argues that current approaches to knowledge security can be overly complicated and lack focus on the social nature of knowledge. For example, employees can keep information relationships with ex-colleagues and there can be a breakdown in traditional structures⁶⁴². The result of this is increased flexibility and access to organisational resources from external entities⁶⁴³. Popescul⁶⁴⁴ proposes using the CIA triad as a solution to engage with these aspects. Popescul⁶⁴⁵ does so to find a balanced solution that allows an organisation to achieve a favourable ratio between openness, protection, and innovation.

Popescul⁶⁴⁶ argues that confidentiality involves ensuring that only authorised persons have access to relevant knowledge, usually in explicit forms. Applicable controls usually focus on

⁶³⁷ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 24.

⁶³⁸ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 24.

⁶³⁹ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 174.

⁶⁴⁰ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 131.

⁶⁴¹ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1338.

⁶⁴² Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1339.

⁶⁴³ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1341-1342.

⁶⁴⁴ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1338.

⁶⁴⁵ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1339.

⁶⁴⁶ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1339.

tangible sources of information; however, this focus can create a tacit paradox⁶⁴⁷. While explicit sources are easiest to secure, if tacit knowledge is not captured and converted to an explicit form, it will be lost, for example, when an employee leaves a company. According to Popescul, employee knowledge should be captured and stored in depositories where possible⁶⁴⁸. Popescul states that integrity involves ensuring that explicit knowledge is “kept in a correct and complete form and must not be modified without consent”⁶⁴⁹. If an employee leaves a company, it can result in a loss of integrity, even when not affecting confidentiality. This is because, they take their relational capital with them, which can result in unbalanced work teams. Protection in this instance must ensure that managers do their best to draw out valuable knowledge from employees and store it⁶⁵⁰. Accessibility focuses on ensuring that access to knowledge resources is given to authorised users at the appropriate time⁶⁵¹. This is important, as cross-organisational and stakeholder collaboration is essential to achieve competitive success. Thus, making knowledge accessible in a secure way is important.

Ilvonen *et al.*⁶⁵² discuss that threats to knowledge can include things like employee turnover, obsolete knowledge, or leaks to competitors. Knowledge security is the managerial process that aims to secure it against these threats. Ilvonen *et al.*⁶⁵³ also outline that the mechanisms of knowledge security can consist of both formal and informal measures. Formal measures focus on KMSs and are aligned with information security. Informal measures focus on KM processes, cultural awareness, and recognition to deal with the human element. Ilvonen *et al.* also suggest using the CIA triad, but there are some differences from Popescul’s approach. Ilvonen *et al.*: emphasise handling integrity issues first and using this as the basis to ensure confidentiality and availability. This is done to improve sharing by minimising knowledge overload and defining which knowledge is of importance, as governed by the CIA triad⁶⁵⁴.

⁶⁴⁷ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1339.

⁶⁴⁸ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1339.

⁶⁴⁹ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1340.

⁶⁵⁰ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1340.

⁶⁵¹ Popescul, 2011. *The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation* p 1340.

⁶⁵² Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4023.

⁶⁵³ Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4023.

⁶⁵⁴ Ilvonen *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4021.

Structural Management Perspective – Ryan⁶⁵⁵ explores “the concept of political engineering in knowledge security” framed through the need to create a knowledge security architect position. Ryan suggests that security bodies recognise the importance of offering information security management certifications. Yet, they do not offer similar training for knowledge security positions. Ryan contends that to manage knowledge security effectively, there is a need to extend training to the development of a knowledge security architect position⁶⁵⁶. A knowledge security architect would need technical skills, legal skills, political engineering skills and decision-making skills, like those of senior executives⁶⁵⁷. According to Ryan, having such skills is important, as the position would form an integral part of the knowledge strategy team of an organisation. Ryan argues that the importance of this role would be to deal with the more difficult broader architectural decisions brought about by the competing intangible needs of managing knowledge security. These can include an organisation’s politics, corporate culture, idea incubation desires, social interests, and employee culture. Additionally, there is often a need to make decisions or implement technology solutions based on less-than-ideal data, which would require engineering management skills.

Harris *et al.*⁶⁵⁸ highlight the need for a standards-based approach for secure data sharing across organisations but do not provide much in the way of practical suggestions. They outline a series of activities for consideration, based on the conflicting need to share data as well as secure it; discussed in terms of the high costs involved to organisations. These activities are broadly focused on the issues of data management, KM, and security management. From a knowledge security perspective, they discuss the need for secure data sharing in KM related to establishing strategies, processes, and metrics for decision support⁶⁵⁹. They also argue that security standards must cover KM aspects too⁶⁶⁰.

Security and Success Factor Perspective – Holsapple and Joshi⁶⁶¹ aim to investigate the key success factors that influence KM. While knowledge security is not the primary focus of the

⁶⁵⁵ Ryan, 2006. *Political Engineering in Knowledge Security* p 265.

⁶⁵⁶ Information Systems Audit and Control Association (ISACA); International Information System Security Certification Consortium (ISC²)

⁶⁵⁷ Ryan, 2006. *Political Engineering in Knowledge Security* p 265.

⁶⁵⁸ Harris *et al.*, 2007. *Standards for Secure Data Sharing Across Organisations* p 86.

⁶⁵⁹ Harris *et al.*, 2007. *Standards for Secure Data Sharing Across Organisations* p 86.

⁶⁶⁰ Harris *et al.*, 2007. *Standards for Secure Data Sharing Across Organisations* p 93.

⁶⁶¹ Holsapple & Joshi, 2000. *An Investigation of Factors that Influence the Management of Knowledge in Organisations* p 235.

paper, it is briefly mentioned as forming part of broader KM success factors. In this regard, one of the key factors for success is control, particularly relating to human, managerial, and financial resources. The authors define control as centred around “ensuring that needed knowledge resources and processors are available in sufficient quality and quantity, subject to required security”⁶⁶². As such, there are two critical issues associated with control. The first is the protection of knowledge resources, which consists of ensuring that said resources are protected against “loss, obsolescence, unauthorised exposure, unauthorised modification, and erroneous assimilation”⁶⁶³. The second is ensuring the quality of knowledge resources, which consists of “controls to govern the quality of knowledge used in an organisation”⁶⁶⁴.

Park⁶⁶⁵ aims to identify the key issues concerning secure KM and to draw consensus among domain experts to accelerate research and development in the field. Park⁶⁶⁶ explains that in terms of the digitalisation of KM, information security does not cover a wide enough range of KM practices. Additionally, researchers have also largely ignored the question of how to secure KM practices effectively. Park argues that while securing knowledge is seen as a barrier to sharing, not securing knowledge can also create a barrier to sharing⁶⁶⁷. The reason Park gives is that a lack of security controls can result in a reluctance “to share knowledge because of the unknown threats associated with industrial espionage”⁶⁶⁸. Additionally, making things too open can also create the potential to overload employees with irrelevant knowledge⁶⁶⁹. Achieving balance is a difficult task, as it is imperative for organisations to remain competitive while still

⁶⁶² Holsapple & Joshi, 2000. *An Investigation of Factors that Influence the Management of Knowledge in Organisations* p 240.

⁶⁶³ Holsapple & Joshi, 2000. *An Investigation of Factors that Influence the Management of Knowledge in Organisations* p 240.

⁶⁶⁴ Holsapple & Joshi, 2000. *An Investigation of Factors that Influence the Management of Knowledge in Organisations* p 240.

⁶⁶⁵ Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 421.

⁶⁶⁶ Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 421.

⁶⁶⁷ Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 421.

⁶⁶⁸ Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 421.

⁶⁶⁹ Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 421.

safeguarding their knowledge resources. Thus, SKM should help to extend the KM concepts, tools, and strategies from a security-driven perspective to achieve this balance⁶⁷⁰.

Jennex and Zyngier⁶⁷¹ explore why security should be viewed as a stronger critical success factor when determining KM success⁶⁷², particularly in KM research⁶⁷³ as integrated into KM success models⁶⁷⁴. For KM to be successful, they outline that it should be focused on capturing the right knowledge, getting it to the right users, and using it to improve performance securely⁶⁷⁵. They suggest that security is not something that is intuitive to KM researchers, where the focus is generally on overcoming barriers to knowledge transfer⁶⁷⁶. Where there is some focus given to security, they highlight that this generally deals with security technologies related to KM systems⁶⁷⁷. Yet, as they argue, having a broader sense of KM security is important, particularly from a governance and integrated model perspective, to mitigate threats targeting critical knowledge⁶⁷⁸. Thus, Jennex and Zyngier⁶⁷⁹ discuss framing security as a KM and governance issue by using a risk management view, combined with the National Security Telecommunications and Information Systems Security Committee model (NSTISSC). They propose doing so by using the model to develop a KM security plan that is not bound by any specific technologies, organisational needs, or characteristics⁶⁸⁰. When applied to KM, the focus of this plan should include management support, leadership, awareness, resource allocation, risk management, strategy, controls, and policies focused on protection, access, and use⁶⁸¹.

⁶⁷⁰ Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 421.

⁶⁷¹ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 403.

⁶⁷² Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 400.

⁶⁷³ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 399.

⁶⁷⁴ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 399.

⁶⁷⁵ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 401.

⁶⁷⁶ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 400.

⁶⁷⁷ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 399.

⁶⁷⁸ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 400.

⁶⁷⁹ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 399.

⁶⁸⁰ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 403-404.

⁶⁸¹ Jennex & Zyngier, 2007. *Security as a Contributor to Knowledge Management Success* p 404.

Mills and Smith⁶⁸² evaluated the impact of specific KM resources, such as KM enablers and processes, on organisational performance. They did this by surveying managers⁶⁸³ to assess the links between specific KM resources and organisational performance⁶⁸⁴. Part of their analysis examined the impact of knowledge protection as a contributing factor to organisational performance⁶⁸⁵. They found that knowledge protection is of statistical significance ($p \leq 0.05$) as a positive contributing factor to organisational performance⁶⁸⁶. Mills and Smith state that “knowledge protection is necessary for effective functioning and control within organisations”⁶⁸⁷. They frame it as focusing on things like copyright and patents as well as IT systems used to handle knowledge. They explain further that there is no “silver bullet”⁶⁸⁸ to enhancing organisational performance and managers need to identify which resources and capabilities will be most effective in their context⁶⁸⁹.

Integration and Research Mapping Perspective - Jennex and Durcikova⁶⁹⁰ posit that there is not a close enough link between information systems security and KM. They contend that this is due to a lack of research and practical interest among practitioners and executives, as it is seen to conflict with knowledge sharing or create difficulties in balancing KM objectives⁶⁹¹. Additionally, if information security issues are considered at all, it is done more as an afterthought⁶⁹². Yet, having such a link, they argue, is important due to the growing reliance on knowledge in organisations and an environment of persistent threats directed towards knowledge assets. The authors suggest that there is a need for KM managers to be more familiar with information security and that it would be beneficial for organisations to develop positions

⁶⁸² Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 156.

⁶⁸³ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 189.

⁶⁸⁴ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 156.

⁶⁸⁵ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 165.

⁶⁸⁶ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 164.

⁶⁸⁷ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 160-161.

⁶⁸⁸ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 160-161.

⁶⁸⁹ Mills & Smith, 2011. *Knowledge Management and Organisational Performance: A Decomposed View* p 167.

⁶⁹⁰ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are we Doing Enough to Thwart the Persistent Threat?* p 1.

⁶⁹¹ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are we Doing Enough to Thwart the Persistent Threat?* p 5.

⁶⁹² Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are we Doing Enough to Thwart the Persistent Threat?* p 5.

focused on SKM. Jennex and Durcikova⁶⁹³ contend that KM governance needs to be integrated more with security policies and standards and that security professionals need to work alongside KM professionals.

4.3.3.4 A Risk Management Paradigm Relating to Knowledge Security in Organisations

In line with the framework discussed above, concerning a ‘Risk Management Paradigm’, three key perspectives were identified from the literature within this general knowledge security categorisation. These are: 1) A Knowledge Retention Perspective. 2) A Balanced Sharing Perspective. 3) An Integrated Knowledge Risk Perspective. These are discussed in the paragraphs to follow.

Knowledge Retention Perspective – The International Atomic Energy Agency⁶⁹⁴ (IAEA) discusses the role of risk management in preventing knowledge loss in nuclear industry organisations. The IAEA explains that such loss can take the form of experts retiring or industry talent being lost in other ways affecting corporate memory and capability. They state that this “poses a clear internal threat to the safe and reliable operation of nuclear facilities”⁶⁹⁵, with the same idea being paralleled to non-nuclear industries. To tackle this problem, the IAEA⁶⁹⁶ proposes using a strategic risk management-based approach “to determine the potential for loss of critical knowledge”⁶⁹⁷, particularly knowledge that is undocumented and would be lost with the departure of experienced industry workers⁶⁹⁸. The IAEA⁶⁹⁹ emphasises that as part of this process, it is also important to include inputs from programmes based around workforce planning, recruitment initiatives, training programmes, succession planning, and leadership development as well as KM components. The reason is that these elements build and feed into an organisation’s broader critical knowledge retention objectives.

As with the IAEA publication, Boyles *et al.*⁷⁰⁰ also examine taking a risk management approach to preventing knowledge loss in nuclear organisations. It appears that the journal publication

⁶⁹³ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are we Doing Enough to Thwart the Persistent Threat?* p 6.

⁶⁹⁴ IAEA, 2006. *Risk Management of Knowledge Loss in Nuclear Industry Organisations* p v.

⁶⁹⁵ IAEA, 2006. *Risk Management of Knowledge Loss in Nuclear Industry Organisations* p v.

⁶⁹⁶ IAEA, 2006. *Risk Management of Knowledge Loss in Nuclear Industry Organisations* p 6.

⁶⁹⁷ IAEA, 2006. *Risk Management of Knowledge Loss in Nuclear Industry Organisations* p 6.

⁶⁹⁸ IAEA, 2006. *Risk Management of Knowledge Loss in Nuclear Industry Organisations* p 4.

⁶⁹⁹ IAEA, 2006. *Risk Management of Knowledge Loss in Nuclear Industry Organisations* p 6.

⁷⁰⁰ Boyles *et al.*, 2009. *Risk Management of Knowledge Loss in Nuclear Industry Organisations* p 126.

by Boyles *et al.* is related to the original IAEA handbook publication, as it follows the same paradigm and recommendations and identifies the same problems and solutions. Thus, they recommend a process, from the position of organisations, consisting of conducting knowledge loss risk assessments to identify specific knowledge loss threats; evaluating the consequences of the loss of critical knowledge and skills; developing action plans to retain critical knowledge; and using this knowledge to improve the skills and competencies of new and existing workers.

Jennex⁷⁰¹ proposes a methodology for organisations to assess the risk of knowledge loss, based on the IAEA approach, should an employee leave. Although the process is the same as that of the IAEA, some additional considerations are mentioned. Jennex⁷⁰² points out that a less thought about aspect of an employee leaving is the strategic impact of losing someone with decades of experience⁷⁰³. This can be detrimental, as it can fundamentally affect the core capabilities of an organisation to perform its objectives, with the subsequent cost, therefore, being much higher⁷⁰⁴. For example, through knowledge worker loss, the capability of energy companies in California was diminished, leading to the 2001-2002 energy crisis in that region⁷⁰⁵.

A further issue raised by Jennex⁷⁰⁶ is the practice of capturing the knowledge of leaving employees. Jennex argues that even when such knowledge is captured, it is not always easily translatable and reusable by new employees as it lacks context and universal application. To counter this, Jennex⁷⁰⁷ proposes that instead of focusing on knowledge at the employee position level, emphasis should rather be placed on the individual skills level. This distinction is needed as most organisations have a project, product or service focus rather than the nuclear industry's focus on systems⁷⁰⁸. As this focus is different, it means that an individual's experience in other industries can vary widely, making it more important to assess the individual rather than the position⁷⁰⁹.

⁷⁰¹ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 189.

⁷⁰² Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 186.

⁷⁰³ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 186.

⁷⁰⁴ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 191.

⁷⁰⁵ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 186.

⁷⁰⁶ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 187.

⁷⁰⁷ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 192.

⁷⁰⁸ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 192.

⁷⁰⁹ Jennex, 2014. *A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel* p 192.

Balanced Sharing Perspective - Ryan⁷¹⁰ highlights the challenges associated with how to manage the tension between knowledge sharing and IP protection. Ryan does so by using a combination of narrative and analysis focused on the importance of return on investment (ROI). This is characterised by risk and managing the transience of knowledge through systems, processes, and partner organisations⁷¹¹. From a security perspective, Ryan⁷¹² outlines the difficulty and complexity associated with trying to manage and secure knowledge in a transient, essentially borderless, environment. Thus, as Ryan⁷¹³ discusses, it is not possible to secure everything and that there needs to be a middle ground when securing knowledge assets. Taking such an approach is important so as not to hinder efficiency, kill innovation or employee morale. To overcome this, Ryan proposes using ROI as a mechanism to calculate the expected benefit of securing knowledge, to the context value of the knowledge being protected.

Integrated Knowledge Risk Perspective – Shedden *et al.*⁷¹⁴, take the view that current KM philosophies are inherently insecure, resulting in the loss of key knowledge through the failure of business processes⁷¹⁵. To counter this, they outline that a supportive control process needs to be in place, that ensures that required knowledge processors and resources are available in enough quality and quantity⁷¹⁶. Also, that they are subject to appropriate security requirements. They continue by outlining that this insecurity has been perpetuated due to the conflicting paradigm between sharing and securing knowledge.

To tackle this challenge, Shedden *et al.*⁷¹⁷ propose incorporating a knowledge perspective into security risk assessments; structured around the Operationally Critical Threat, Asset, and Vulnerability Evaluation – Small (OCTAVE-S) methodology. Currently, applying information security based approaches to assess knowledge risk directly is problematic, as it may obscure key risks associated with the cultivation and deployment of organisational knowledge⁷¹⁸. This is because information security risk assessments focus on the tangible, while knowledge can be intangible too. For example, while typical information security methodologies identify

⁷¹⁰ Ryan, 2006. *Managing Knowledge Security* p 143.

⁷¹¹ Ryan, 2006. *Managing Knowledge Security* p 143.

⁷¹² Ryan, 2006. *Managing Knowledge Security* p 143.

⁷¹³ Ryan, 2006. *Managing Knowledge Security* p 144.

⁷¹⁴ Shedden *et al.*, 2011. *Incorporating a Knowledge Perspective into Security Risk Assessments* p 5.

⁷¹⁵ Shedden *et al.*, 2011. *Incorporating a Knowledge Perspective into Security Risk Assessments* p 2.

⁷¹⁶ Shedden *et al.*, 2011. *Incorporating a Knowledge Perspective into Security Risk Assessments* p 3.

⁷¹⁷ Shedden *et al.*, 2011. *Incorporating a Knowledge Perspective into Security Risk Assessments* p 2.

⁷¹⁸ Shedden *et al.*, 2011. *Incorporating a Knowledge Perspective into Security Risk Assessments* p 1.

people as critical assets, consideration also needs to be given to detailed accounts of individual knowledge, collective knowledge, and their relationship to organisational processes⁷¹⁹.

Padyab *et al.*⁷²⁰ discuss too how risk methodologies like OCTAVE-S fail to address knowledge security issues adequately. They argue that it is in part due to the focus on organisational processes as technical activities, combined with a lesser focus on the organisational dynamics of information management and knowledge sharing⁷²¹. Thus, as they explain, knowledge can be at risk in situations where it is shared outside of the technical realm, between people and the organisation⁷²². Additionally, knowledge sharing may concern both tacit and explicit knowledge and involve the knowledge creation modes of SECI as outlined by Nonaka.

As a solution, Padyab *et al.*⁷²³ propose using a genre-based approach to assess information and knowledge security risks. The objective is to orientate the risk assessment methodology toward a knowledge-centric paradigm. Padyab *et al.* discuss that this can be done by using the genre-based analytical method or identifying organisational communication patterns through which knowledge is shared. According to Padyab *et al.*⁷²⁴, a genre of organisational communication is a typified communicative action invoked in response to a recurrent situation. Additionally, genres can also “capture”⁷²⁵ information regarding business practices that are undocumented, existing in people’s minds and communication habits⁷²⁶. Taking such an approach, as Padyab *et al.*⁷²⁷ argue, is useful as communication patterns are viewed as the basis for mapping knowledge sharing and the related knowledge sharing security risks.

Thalmann *et al.*⁷²⁸ contend that there has been a lack of focus on knowledge protection, as opposed to sharing, in both the literature and practice. As a result, they suggest that when attention is given to protecting data and information, not understanding the balance between sharing and protection, could result in a rigid implementation. Rigidity, in this instance, means

⁷¹⁹ Shedden *et al.*, 2011. *Incorporating a Knowledge Perspective into Security Risk Assessments* p 1.

⁷²⁰ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 14.

⁷²¹ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 13.

⁷²² Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 14.

⁷²³ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 13.

⁷²⁴ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 16.

⁷²⁵ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 16.

⁷²⁶ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 17.

⁷²⁷ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 14.

⁷²⁸ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 29.

that the related goals are thought about in a non-systematic way. Similarly to Padyab *et al.*, they outline that, while IT security management (ITSM) already proposes frameworks, guidelines, and modes⁷²⁹, explicit knowledge is not stored in physical IT systems alone. Rather, it is exchanged via social software or media and is difficult to protect by traditional ITSM. Further, the implicit knowledge stored within organisational IT, employees and the transfer pipeline needs to be protected too⁷³⁰. Thus, Thalmann *et al.*⁷³¹ suggest developing an integrated risk management framework. They outline that the framework should be developed holistically, by incorporating risk management, ITSM, performance measurements and KM, covering both the technical and non-technical elements embedded in processes and systems⁷³². Technical aspects are associated with process mining techniques, governed by the interaction between the different elements. Non-technical aspects are those associated with processes⁷³³.

Thalmann *et al.*⁷³⁴ point out that a key aspect of this approach is to combine the framework with measuring the success of organisational KM and knowledge protection. Additionally, to identify and assess the associated risks and suggest controls to help reduce these⁷³⁵. In this instance, measurement is aligned with a structured ITSM approach used to gauge things like compliance to standards, guidelines, frameworks, etc., through the knowledge auditing process⁷³⁶. Thalmann *et al.*⁷³⁷ suggest that using a measured approach to knowledge protection allows an organisation to gauge the effectiveness of the controls and performance of the knowledge protection measures they put in place⁷³⁸.

⁷²⁹ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 29.

⁷³⁰ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 33.

⁷³¹ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 23.

⁷³² Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 31-33.

⁷³³ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 28.

⁷³⁴ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 28.

⁷³⁵ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 31.

⁷³⁶ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 28.

⁷³⁷ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 33.

⁷³⁸ Thalmann *et al.*, 2014. *An Integrated Risk Management Framework: Measuring the Success of Organisational Knowledge Protection* p 33.

4.3.3.5 Examining the Balance of Categories

Upon examining the literature presented in Table 4-5, there is a clear research focus orientated towards issues related to systems security (18 texts), assurance (11 texts) and risk management (7 texts), with DIS (2 texts) bringing up the rear. The balance of focus appears to be aligned with the growth in the importance of information security elements for organisations⁷³⁹ and their application to the KM paradigm. In addition, there appears to have been several key driving factors from within the knowledge security research community that have contributed to this balance.

Firstly, relating to the focus on the ‘Systems and Security Paradigm’, this appears to be because of the outcomes of a series of conferences and workshops on secure KM, originating in the mid-2000s. The primary event associated with this development was *The First Secure Knowledge Management Workshop* which took place in 2004⁷⁴⁰. As part of the proceedings of the workshop, Park *et al.* conducted a Delphi Study on a sub-group of the participants and interested parties. They did this to determine the key issues that would need to be thought about in terms of developing a coherent research agenda⁷⁴¹, related to knowledge security. The results of the analysis by Park *et al.* have been summarised in Table 4-6 and include 18 important areas related to secure KM⁷⁴².

Upon examination of the 18 important areas, it is apparent that these issues framed the research focus of knowledge security in a very technically driven, systems focused way. This approach can be seen in the other research papers stemming from *The Second Secure Knowledge Management Workshop*⁷⁴³, where most took a systems security focus. For example, Memon and Daniels, who participated in the second workshop, state that “security is a major issue

⁷³⁹ Zurich Insurance Group, 2015. *Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures* p 11.

⁷⁴⁰ Park *et al.*, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 422.

⁷⁴¹ Park *et al.*, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 422.

⁷⁴² Park *et al.*, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 423.

⁷⁴³ Memon & Daniels, 2007. *Special Issue on Secure Knowledge Management* p 449.

revolving around KMSs⁷⁴⁴, thus reinforcing a technically driven⁷⁴⁵ KMS or semantic web security paradigm.

Table 4-6: Ranking of Important Issues in Secure KM Research by Park *et al.*

Key Research Issues by Rank	
1.	Developing access controls and policies for organisational knowledge
2.	Datamining/utilisation techniques under security and privacy considerations
3.	Understanding economics of knowledge sharing and information security investment
4.	Designing and developing techniques for SKM systems and secure content management
5.	Adopting semantic web for interoperable KM system/integration of KM across heterogeneous systems
6.	Advances in information privacy
7.	Understanding economics of knowledge markets
8.	Aligning business policy, business processes and SKM policy
9.	Improving knowledge representation
10.	Developing trust management mechanisms for networked systems
11.	Securely managing knowledge at the data level
12.	Exploring the roles and implications of government in information security
13.	Developing mechanisms to effectively handle vulnerability/threat responses
14.	Improving interaction between security mechanisms and their users
15.	Improving effectiveness of secure systems
16.	Developing self-defending/healing mechanism in computer systems
17.	Developing metrics for SKM productivity and improving KMS productivity
18.	Secure KM for wireless services

From this view, the technical focus of the research seems to correlate with technology being the driving force for KMSs⁷⁴⁶. Since the system aspects relating to the functioning of a KMS are almost always technically focused, it can be argued that it creates a need for technically orientated solutions; as with the focus of cyber security driven solutions⁷⁴⁷. Further, it is also likely due to there being more complicated issues associated with KMSs when it comes to

⁷⁴⁴ Memon & Daniels, 2007. *Special Issue on Secure Knowledge Management* p 449.

⁷⁴⁵ Memon & Daniels, 2007. *Special Issue on Secure Knowledge Management* p 449.

⁷⁴⁶ Maier, 2005. *Knowledge Management Systems: Information and Communication Technologies for Knowledge Management* p 273-274.

⁷⁴⁷ Beard, 2019. *Harvard Business Review: Why Cybersecurity Isn't Only a Tech Problem* [Online].

managing access rights, as opposed to traditional information systems⁷⁴⁸. In addition, there is also the complexity of needing to validate the knowledge and documents contained in these systems⁷⁴⁹. Thus, there is a large variety of complexity associated with defining who has access to what knowledge resources across teams and how this access is granted and managed when conflicting requirements occur⁷⁵⁰. Since these are driven by ICTs⁷⁵¹, it makes sense that there would be an interest in researching solutions as to how this can be achieved autonomously. The objective is to relieve the cognitive load on IT personnel as mentioned previously⁷⁵². The combination of the direction of the research focus, the increased reliance on technical mechanisms and the upswing in the criticality of cyber security related issues in organisations, seems to have set the stage for the research focus followed. When examining the more recently listed workshop domains of the *Secure Knowledge Management Workshop*⁷⁵³ from 2017, there was still a strong focus on technical approaches to KM and KMS issues. For example, some of the domains listed on the conference website include issues relating to cloud computing, big data, the internet of things, cyber-physical systems, data mining, threat detection and so on⁷⁵⁴, all of which hold a similar technical focus to more recent developments in the cyber technical framework as it relates to KM and KMS issues.

Secondly, relating to the focus on the ‘Assurance Paradigm’ and ‘Risk Management Paradigm’, these appear to be consistent with the increased general research focus into organisational information security, assurance, and risk issues. These issues have increased in importance from the mid-2000s onwards, seemingly correlating with the rise in the importance of information and knowledge from an economic perspective. From an organisational perspective, this too aligns with the growth in demand for information security, as indicated by the increased spending on cyber security in both the corporate and public sectors⁷⁵⁵. Having this focus appears to create something of a feedback loop into increased research related to these topics

⁷⁴⁸ Ruiz *et al.*, 2011. *A Framework and Implementation for Secure Knowledge Management in Large Communities* p 1-3.

⁷⁴⁹ Ahmad & Ewe, 2005. *A Model for Secure Knowledge Sharing* p 1-4.

⁷⁵⁰ Ahmad & Ewe, 2005. *A Model for Secure Knowledge Sharing* p 1-4.

⁷⁵¹ Maier, 2005. *Knowledge Management Systems: Information and Communication Technologies for Knowledge Management* p 273-274.

⁷⁵² Arora, 2006. *Autonomic-Computing Approach to Secure Knowledge Management: A Game-Theoretic Analysis* p 487.

⁷⁵³ CSIAC, 2017. *Secure Knowledge Management Workshop 2017 (SKM 2017)* [Online].

⁷⁵⁴ CSIAC, 2017. *Secure Knowledge Management Workshop 2017 (SKM 2017)* [Online].

⁷⁵⁵ Zurich Insurance Group, 2015. *Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures* p 11.

in academia. In turn, reflecting on the popularity of the research interests into KM and the framing of knowledge security from a security, assurance, and risk-based view. The research focused on systems security, assurance and risk issues seem to relate to those aspects outlined by Park *et al.* as most urgent to deal with⁷⁵⁶. In this regard, Park *et al.* found the most important issues to be “developing access controls, policies, advances in information privacy and designing and developing techniques to secure KMSs and to secure their contents”⁷⁵⁷. According to Park *et al.*, these issues also need to align with business policy, processes, privacy issues, and knowledge security policy. Thus, this requires research focused on both technical and non-technical security issues.

Finally, relating to the smaller focus on the ‘DIS Paradigm’ as applied to commercial organisations, this appears to have been driven by the work of Desouza⁷⁵⁸. Fitz-Gerald⁷⁵⁹ argues that this is a more controversial approach to take, as the DIS view is based on counterintelligence principles and other DIS based security mechanisms⁷⁶⁰ as a means of securing knowledge in commercial organisations. Therefore, such approaches do not fit with the traditional information security, assurance or risk research agendas of most knowledge security authors. However, even though taking such an approach to knowledge security in commercial organisations is less popular, it is still of value⁷⁶¹ and could be considered something of an under-researched area. This becomes evident when facing competitive intelligence gathering, which employs a different array of tactics beyond the realm of systems security, assurance, or risk tools. Thus, they may not be adequately placed to deal with such threats, and it is not necessarily a true reflection of a DIS approaches potential value in securing organisational knowledge.

⁷⁵⁶ Park *et al.*, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 425.

⁷⁵⁷ Park *et al.*, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 425.

⁷⁵⁸ Desouza, 2007. *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* p 85-99.

⁷⁵⁹ Fitz-Gerald, 2008. *Review: Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets*, K.C. Desouza p 342.

⁷⁶⁰ Desouza & Vanapalli, 2005. *Securing Knowledge in Organizations: Lessons from the Defence and Intelligence Sectors* p 89.

⁷⁶¹ Fitz-Gerald, 2008. *Review: Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets*, K.C. Desouza p 342.

4.5 Conclusion

Chapter 4 formed the third and final part of the theoretical analysis and aimed at outlining what security approaches are expressed in the literature that focus on KM, how they can be categorised and why there is a need for knowledge security. This was in line with the research questions as illustrated in Chapter 1, Figure 1-2⁷⁶² ⁷⁶³. Thus, the objective of Chapter 4 was to provide an overview of the security literature relating to what security dimensions are expressed therein, keeping the KM paradigm in mind. I did this by firstly establishing context, through examining the need to integrate knowledge security with KM and the need for knowledge security in organisations. Next, the literature was examined in detail based on a process of identification and categorisation. The result of this process allowed for the identification of key paradigms and perspectives from within the body of literature, as relating to securing knowledge in organisations. Finally, a brief analysis was given as to the possible reasons for the most common paradigmatic focuses from the literature in terms of examining the balance of the categories. Chapter 5 will examine knowledge security in teaching and academic programs. I will do this to relate knowledge security activity to the industry perspective, to provide as complete a picture as possible for the conceptual model inputs. This will form the first part of the empirical analysis and pertains to the research objective of examining if knowledge and security are treated as separate entities in the teaching and academic programs at leading universities.

⁷⁶² Research sub-question 4.1: *What security approaches are expressed in the literature that focus on KM and how can they be categorised?*

⁷⁶³ Research sub-question 4.2: *Why is there a need for knowledge security?*

Part 2 – Empirical Analysis

Chapter 5

Review of Knowledge Security in Leading Academic Programs

5.1 Introduction

The chapter deals with the first part of the empirical component of the study following an open-access approach. Thus, it consists of a review of whether knowledge and security are treated as separate entities in the teaching and academic programs of leading universities in the field of information science and studies. This approach is premised on the view that what is taught at leading universities will provide a representation of what the state of the art is and thus what is being pursued in organisations. The initial assumption is that security and KM are treated as separate areas in academia and will be treated as separate areas in practice. It sets the foundation to confirm or deny this in the second part of the empirical component of the study, examined in Chapter 6, and to help provide further inputs for the development of the conceptual model outlined in Chapter 7. The chapter begins by firstly outlining how the leading universities were identified. This is followed by an overview of the approach used to review these leading universities, to establish the relationship between KM and security, if any. Finally, the findings of the analysis are discussed, as they relate to each university, and a discussion of the overall findings is given.

5.2 Identifying Relevant Universities

The first task of the investigation was to identify and compile a list of relevant universities. The objective here was not to identify the teaching and academic activities relating to KM and security at all universities. Rather, it was to examine if the selected leading universities in the field of information science and studies conducted such activities and to establish if these were integrated or not. For this purpose, five universities in the United States of America (USA) and five in the European Region (EUR), who are perceived to be academic leaders in the field of information science and studies, were chosen. There are several reasons for focusing on the

USA and EUR regions. Firstly, these regions are perceived to be at the forefront of having to deal with security threats. For example, according to the Malwarebytes Lab⁷⁶⁴, the USA and EUR regions have the highest level of threat detections by their software. Secondly, according to the International Monetary Fund (IMF)⁷⁶⁵, the USA and EUR regions contain 11 of the 20 biggest economies in the world. Thirdly, based on the World Bank's Knowledge Economy Index (KEI), which is derived from the four pillars related to the knowledge economy⁷⁶⁶, 16 of the top 20 countries listed (last available data from 2012) are found in these regions. Fourthly, according to the Times Higher Education (THE) World University Rankings⁷⁶⁷, based on 13 performance indicators which include teaching, research, and knowledge transfer, 19 of the top 20 universities listed are found in these regions. Thus, assuming based on these factors that how leading universities in these regions handle the concept of knowledge security will reflect the state of the art as it currently stands in academic training and, therefore, how it translates into practice.

5.2.1 The Identification Process

The identification of the institutions was done based on the use of rankings systems relevant to information science and studies. Although several ranking bodies were examined⁷⁶⁸, not all were deemed to be relevant for this investigation because some rankings were too broad in their approach, either listing only broad concepts like "IT", or only drilled down to a faculty level, such as "Humanities". As the rankings used needed to be relevant to information science and studies, I eliminated those that did not have a specific focus on these areas. Thus, I was left with the following rankings: 1) U.S. News & World Report for Library & Information Science and Studies Rankings. 2) Quacquarelli Symonds (QS) rankings for Library and Information Management. 3) Academic Ranking of World Universities for Library and Information Science and Studies.

⁷⁶⁴ Malwarebytes Labs, 2020. *State of Malware Report - 2020* p 6.

⁷⁶⁵ IMF, 2020. *IMF Data Mapper, GDP - Current Prices* [Online].

⁷⁶⁶ Wikipedia, 2019. *Knowledge Economic Index* [Online].

⁷⁶⁷ Times Higher Education, 2020. *World University Rankings 2020* [Online].

⁷⁶⁸ Examples of the university ranking bodies considered include: The National Taiwan University Rankings, Leiden Ranking, Webometrics, CHE University Rankings, European Classification of Higher Education Institutions, Multirank University and College Rankings, U.S. News & World Report Rankings, Cybermetrics Lab Rankings, Academic Ranking of World Universities (Shanghai Rankings), University Ranking by Academic Performance, The Times Higher Education World University Rankings, Clarivate Analytics Rankings and The Quacquarelli Symonds University Ranking.

While university rankings are perceived to be somewhat controversial, I decided that they were still suitable for use in the objectives of this research. My justification is that the objective was not to get an absolute definitively ranked and ordered list, where the position would be important, but rather to identify a general array of factors that related to the institutions that are seen to be leaders in the field. As an additional check to see that the rankings were representative of information science and studies, and as a precursor to the filtering and selection of the final five universities in each region, I also cross-checked the ranking lists with the iSchools organisation members list.

The iSchools organization was founded in 2005 by a collective of Information Schools dedicated to advancing the information field in the 21st Century. The organization incorporated as iSchools Inc. in 2015 and was granted 501(c)(3) non-profit status by the IRS in 2016. These schools, colleges, and departments have been newly created or are evolving from programs formerly focused on specific tracks such as information technology, library science, informatics, and information science/studies. While each individual iSchool has its own strengths and specializations, together they share a fundamental interest in the relationships between information, people, and technology⁷⁶⁹.

While not a completely representative list of all information science and studies institutions, it was useful to check if most of those institutions found were listed there too. Of my list of preliminarily identified institutions from the rankings for the USA, 75% were also listed on the iSchools organisation database and 37.5% for the EUR region. As the iSchools organisation was founded in the USA, the higher representation of US universities made sense with the 37.5% from the EUR region being proportional to their lower representation in the database. Through the filtering and aggregation process, I aimed to further refine my list by using the iSchools group as a representative filter, as discussed in the section to follow. The list of identified institutions per ranking body is shown in Table 5-7. This consists of the ranking body, the year of the ranking, the region from which the universities are from and the universities as listed by the ranking bodies.

⁷⁶⁹ iSchools, 2020. *About the iSchools Organisation* [Online].

Table 5-7: List of Identified Institutions per Ranking Body

Ranking Body	Year	University
United States of America		
U.S. News & World Report – Library & Information Science and Studies Rankings ⁷⁷⁰	2017	<ul style="list-style-type: none"> • University of Illinois, Urbana-Champaign • University of Washington • University of North Carolina, Chapel Hill • Syracuse University • University of Michigan, Ann Arbor
Quacquarelli Symonds – Library & Information Management Rankings ⁷⁷¹	2020	<ul style="list-style-type: none"> • University of North Carolina, Chapel Hill • University of Illinois, Urbana-Champaign • University of Washington • Syracuse University • Indiana University Bloomington
Academic Ranking of World Universities – Library & Information Science and Studies Rankings ⁷⁷²	2019	<ul style="list-style-type: none"> • Harvard University • University of Michigan, Ann Arbor • Indiana University Bloomington • Vanderbilt University • University of Washington
Europe		
Quacquarelli Symonds – Library & Information Management Rankings ⁷⁷³	2020	<ul style="list-style-type: none"> • University of Sheffield • Loughborough University • University of Amsterdam • Tampere University • University College of Borås
Academic Ranking of World Universities – Library & Information Science and Studies Rankings ⁷⁷⁴	2019	<ul style="list-style-type: none"> • University of Amsterdam • University of Wolverhampton • KU Leuven • University of Granada • University of Sheffield

⁷⁷⁰ US News & World Report, 2017. *Best Library and Information science/studies Programs* [Online].

⁷⁷¹ QS World University Rankings, 2020. *Library and Information Management* [Online].

⁷⁷² Academic Ranking of World Universities, 2019. *Shanghai Ranking's Global Ranking of Academic Subjects 2019 - Library and Information science/studies* [Online].

⁷⁷³ QS World University Rankings, 2020. *Library and Information Management* [Online].

⁷⁷⁴ Academic Ranking of World Universities, 2019. *Shanghai Ranking's Global Ranking of Academic Subjects 2019 - Library and Information science/studies* [Online].

5.2.2 The Filtering and Aggregation Process

Upon completing the compilation of the list, I moved on to conduct a process of filtering and aggregation to determine the final five universities chosen for each region. To do this, I used my spreadsheet software's "Conditional Formatting" function to eliminate duplicates. After doing so, I was left with a list of eight universities for both the USA and EUR regions. To cut the list of identified universities down to the final five, I proceeded to rank the remaining entries on the list further according to five selected criteria: 1) If they have an iSchools listing. 2) The most recent year they appeared on a ranking list. 3) How often they appeared on my chosen rankings' lists. 4) If they had an information science and studies related department in their university. 5) If there was a website available for their information science and studies related university or department and if it was available in English. For each of these elements, I assigned a score. One point was assigned for each element listed and one point for each time the listing appeared in my chosen rankings list, to keep its weighting relative to the other criteria's scores, as shown in Table 5-8.

In terms of my selection of the different criteria, the iSchools listing was chosen as it helps to identify more reputable universities in the field and thus adds some validity to the universities included on my list. The criterion of year was chosen where more recent 2020 listings were favoured. I assigned a point for any university that appeared in a 2020 ranking list as this indicates a more recent representation of their listed ranking. The listed frequency in my selected rankings lists was chosen as a factor in that those universities that appear more on the rankings' lists are likely to be more representative of being leading institutions in the field based on the criteria of the different lists. Having an information science and studies orientated department was chosen as a criterion, as it seems indicative of a more formal academic and teaching focus in the field, where special attention has been assigned to information orientated studies within the respective university. Finally, having an English version of the relevant universities websites was chosen as important, as some universities are in non-English speaking countries. As, it would not be easy for me to search their teaching and academic content in this regard if there was not an English version available. The final five universities chosen for each region that were analysed, in no order, are presented in Table 5-9.

Table 5-8: Filtering Matrix Used to Select the Final Universities for Analysis

University	iSchools	Year	List Frequency	Info Studies	Website	Score
United States of America						
Washington	Yes	2020	3	Yes	Yes	7
Indiana Bloomington	Yes	2020	2	Yes	Yes	6
Syracuse	Yes	2020	2	Yes	Yes	6
Illinois, Urbana- Champaign	Yes	2020	2	Yes	Yes	6
North Carolina, Chapel Hill	Yes	2020	2	Yes	Yes	6
Michigan, Ann Arbor	Yes	2019	2	Yes	Yes	5
Harvard	No	2019	1	No	No	1
Vanderbilt	No	2019	1	No	No	1
Europe						
Sheffield	Yes	2020	2	Yes	Yes	6
Amsterdam	Yes	2020	2	Yes	Yes	6
Borås	Yes	2020	1	Yes	Yes	5
Tampere	Yes	2020	1	Yes	Yes	5
Loughborough	No	2020	1	Yes	No	3
Granada	No	2019	1	Yes	No	2
KU Leuven	No	2019	1	No	No	1
Wolverhampton	No	2019	1	No	No	1

Table 5-9: Aggregated Lists of USA and EUR Universities

United States of America	Europe
<ul style="list-style-type: none"> • Indiana University Bloomington • Syracuse University • University of Illinois, Urbana-Champaign • University of North Carolina, Chapel Hill • University of Washington 	<ul style="list-style-type: none"> • University of Sheffield • Tampere University • University of Borås • University of Amsterdam • Loughborough University

5.3 Analysis of Selected Universities

For my investigation into what is taught at leading universities with regards to information science and studies, I aimed to cover as broad a scope as possible. To do so, I decided to follow a competitive intelligence gathering approach based on open-source intelligence gathering (OSINT)⁷⁷⁵, whereby I searched each university's website for all public information available relating to the concept of knowledge and security. Any findings identified because of this process were then captured in a spreadsheet to be able to discuss and analyse them further as needed. The approach used was thus qualitative, as the material being examined relied on personal knowledge and insight and was not based on capturing statistics relating to the occurrences of the terms or some other form of statistical relationship.

The terms used to search the relevant websites were identified from the texts examined for the literature review as carried out in Chapter 4. I did so, as I considered that this would be indicative of the accepted terms relating to the concept of knowledge security if it were being taught in any of the universities being investigated. When I initially classified the original texts in Chapter 4, apart from assigning the texts a reference code relating to their area of focus, I also assigned a reference code relating to the key semantic terms used in the texts. This was in terms of how the texts referred to the concept of knowledge and security. I then took these results and processed them, again using spreadsheet software, into a list of the most common terms found in the literature. The list of commonly identified terms/phrases relating to knowledge and security from the literature review conducted in Chapter 4 are as follows:

1. Secure Knowledge Management,
2. Knowledge Security,
3. Knowledge Protection,

⁷⁷⁵ CIA, 2010. *Intelligence: Open-Source Intelligence* [Online].

4. Knowledge Loss,
5. Knowledge Retention and
6. Secure Knowledge Sharing.

When compiling the terms, I aimed to avoid listing abbreviations. I did so as using abbreviations would run the risk of cluttering the search results with irrelevant information as abbreviations can mean different things in different fields of study. I, therefore, focused on using whole search terms, as I assumed that these would appear in any related material on the universities' websites in full format at least once.

Commencing with the searches, I decided to use Google Advanced Site Search to search each of the listed universities' websites. I did so, as it allowed for a faster more comprehensive search to take place of the whole website, rather than manually exploring each page on an information orientated department's website. To conduct the search, I thus focused on using each university's domain name, as part of the advanced search criteria, to keep the scope broad. I took such an approach to cover any potential cross-departmental collaborations, or research being done by research centres in addition to the primary information science and studies focused departments. The relevant information science and studies focused departments were thus also covered by using this broad approach as it included any subdomains in the search results too. The site search was based on the search formulation of 'Your Term Here site:yoursitehere.edu'. This was a valid approach to take, as doing so also covered any relevant subdomains falling under the root domain searched. For example, domains such as 'name.yoursitehere.edu' or 'yoursitehere.edu/name'.

Before commencing with the search, I also checked to see that each university site searched had the same root domain for their departmental websites. I took this approach to ensure that the relevant subdomains used were covered by the root domain and that the domains for certain parts of their websites were not completely different. I found only one instance where some course information was stored under a different domain name, which was not a subdomain of the root domain, while the main department and university sites were stored as subdomains under the university's root domain. For example, where a university website was listed in the format 'yoursitehere.edu' and part of the course information listed fell under a different domain name such as 'differentsitename.com'. Fortunately, there was only one such difference found, that being for the University of Washington, where some course module information was stored under a different domain name, and I thus integrated the findings from the two different domain

searches into a single representation of the findings. As I conducted the searches, any relevant information was captured in the spreadsheet as the process progressed to write it up later.

Once the search results had been returned by Google Advanced Site Search, I manually filtered the results. I did this by reading the different page titles listed and examining the page descriptions relating to the context of their highlighted key terms. Pages that appeared to be relevant to what I was searching for, I opened in new tabs and used my browser's built-in search function to search for the keywords from the original search terms used. So, for example, if I had searched for the term 'Knowledge Security' and I found a page that I considered to be relevant, I then opened that page in a new tab and searched for the phrases and words 'Knowledge Security', 'Knowledge' and 'Security'. If a word or term was found on the relevant page, I read the text around it to determine if it had something to do with my topic of interest or was used in a different context. I read the titles and, where possible, the descriptions/abstracts, for each page to gain more context. I also drilled down further into any relevant links found on the pages that I examined as relating to my identified search terms to look for possible additional information.

I continued this manual process for the first five pages of the Google Advanced Site Search results delivered per search term used. I did so as I generally found beyond this point results started repeating or were not relevant to my original search term used any longer. If a term was still delivering relevant results on page five, I then continued several pages further until I found that results were repeating or were no longer relevant to my original search term used. With this investigative process in mind, an overview of the information relating to the different universities targeted will now be discussed in more detail in the two sections to follow. I will begin by discussing the results for the USA universities followed by the results for the EUR universities. This will be done in brief, and I will only outline those elements where some relationship between knowledge and security in teaching and academic programs for the various universities was found.

5.3.1 USA Universities Results and Findings

Indiana University Bloomington – In terms of the relationship between knowledge and security present in the academic programs at the university, while there was no direct reference, the closest I could find was activity related to the protection of IP from a legal perspective, when searching for the term 'Knowledge Protection'. This dealt with elements such as trademarks, trade secrets, copyrights, patents, rights of publicity, licensing, biopharma, e-

commerce, internet law, social media and more⁷⁷⁶. There was no direct mention of teaching or research related to the search terms/phrases of ‘Secure Knowledge Management’, ‘Knowledge Security’, ‘Knowledge Loss’, ‘Knowledge Retention’ or ‘Secure Knowledge Sharing’.

Syracuse University – As with Indiana University Bloomington, there was no direct reference to the relationship between knowledge and security in academic programs at the university. The closest I could find in this instance was also activity related to the protection of IP from a legal perspective; this when searching for the term ‘Knowledge Protection’. Again, this dealt with elements such as patents, policies, trade secrets, copyright, trademarks, internet law and more⁷⁷⁷. There was also no direct mention of teaching or research related to the search terms/phrases of ‘Secure Knowledge Management’, ‘Knowledge Security’, ‘Knowledge Loss’, ‘Knowledge Retention’ or ‘Secure Knowledge Sharing’.

University of Illinois, Urbana-Champaign – When searching for the term ‘Secure Knowledge Management’, there was some evidence of an awareness of security being important for KM activities, but not as a directly taught subject. In one of the courses taught at their iSchool, they outline that they aim to explore “information knowledge management strategies”⁷⁷⁸. The description given outlines things like building effective KM strategies and examining technologies for KM. They combined this with topics like information governance and standards which would imply some level of consideration for security issues, at least from an information systems security perspective. Unfortunately, a deeper breakdown of the syllabus was only available with login credentials. There were some historic indications of interest in the subject whereby I found a 2011 doctoral dissertation by Cho⁷⁷⁹, that dealt with KM and organisational performance. As part of the analysis in the dissertation, Cho wrote briefly about the role and implication of secure KM as a contributing factor to organisational performance. There was also a news article, found on the university website, from 2014⁷⁸⁰ that commented on a former doctoral student from the university who had won a prize for their cloud-sharing start-up which aimed to integrate researchers’ workflows to allow for secure KM and collaboration.

⁷⁷⁶ Indiana University Bloomington, 2020. *Centre for Intellectual Property Law and Innovation* [Online].

⁷⁷⁷ Syracuse University, 2020. *Syracuse Intellectual Property Law Institute* [Online].

⁷⁷⁸ University of Illinois, 2020. *Illinois School of Information Science/Studies – The iSchool at Illinois: IS 590IK Explore Information Knowledge Management Strategies* [Online].

⁷⁷⁹ Cho, 2011. *Knowledge Management Capabilities and Organizational Performance: An Investigation into the Effects of Knowledge Infrastructure and Processes on Organisational Performance* p 57-58.

⁷⁸⁰ Cation, 2014. *Rithmio, AVriculture, and Inscites Win Big at 2014 Cozad Competition* [Online].

When searching for the term ‘Knowledge Protection’, again as with other universities on this list, there was information dealing with courses and research relating to IP protection from a legal standpoint⁷⁸¹. There was also some mention of IP issues from a previously conducted economics course on the economics of innovation and technology⁷⁸². These courses dealt with the same kind of content as the examples listed earlier. When searching for ‘Knowledge Retention’, while again providing no direct evidence of teaching related to this term, there was some evidence of interest in the topic when examining the legacy research interests of certain academic staff of the university. For example, Foss and Mahoney⁷⁸³ explored knowledge governance with an element that focused on knowledge retention. When discussing employees’ acceptance of KMSs and their impact on creating learning organisations, Yoo and Huang⁷⁸⁴ mentioned that organisations are eager to become learning organisations to contribute to the retention of workers who possess valuable organisational knowledge, in addition to some other factors. Finally, in Burnette’s⁷⁸⁵ research paper examining the nature of tacit knowledge sharing among library colleagues in the context of a mentor/mentee relationship, she mentions that an objective of their research was to help inform future tacit knowledge retention efforts that are lacking in many libraries. Thus, while appearing not to be a formal course, this does indicate some awareness of the issue at least on a fringe level. There was no direct mention of teaching or research related to the concepts of ‘Knowledge Security’, ‘Knowledge Loss’ or ‘Secure Knowledge Sharing’.

University of North Carolina, Chapel Hill – For the terms ‘Secure Knowledge Management’ and ‘Knowledge Protection’, there was no direct evidence related to courses being taught in this regard. The only information that came up in the search was that related to IP protection and security which was driven from an IT systems and leadership perspective as per previous short courses held in 2015⁷⁸⁶. Reference to IP was also found in the university’s law school and was offered as a clinic course⁷⁸⁷. The content of the courses was like those discussed relating

⁷⁸¹ University of Illinois, 2020. *Illinois College of Law: Intellectual Property and Technology Law* [Online].

⁷⁸² Chalioti, 2014. *Econ 483: Economics of Innovation & Technology* p 1-7.

⁷⁸³ Foss & Mahoney, 2010. *Exploring Knowledge Governance* p 93-101.

⁷⁸⁴ Yoo & Huang, 2013. *Employees’ Acceptance of Knowledge Management Systems and its Impact on Creating Learning Organizations* p 434-454.

⁷⁸⁵ Burnette, 2017. *Tacit Knowledge Sharing Among Library Colleagues: A Pilot Study* p 382-397.

⁷⁸⁶ University of North Carolina, 2015. *School of Information and Library Science: Special Course Topic Archive* [Online].

⁷⁸⁷ University of North Carolina, 2020. *School of Law: Intellectual Property Clinic* [Online].

to other universities already mentioned and dealt with elements such as patents, copyright and more.

When searching for the term ‘Knowledge Loss’, no specific evidence was found course-wise that would not fit within normal information systems or KMS courses or thinking. There was some mention of preventing knowledge loss through archival processes in some appointment interviews⁷⁸⁸ and guest lectures, but this appeared to be framed more from an information and library perspective or to achieve knowledge preservation for open access purposes⁷⁸⁹ rather than as an organisational security concern. In terms of the term ‘Knowledge Retention’, there was also no direct evidence found course-wise that focused specifically on the issue of knowledge retention for security purposes. There were some historical references from a health informatics research seminar relating to knowledge retention found from an IT systems perspective or as part of a knowledge retention strategy⁷⁹⁰. From an HR perspective, there were some course references relating to the importance of retaining staff⁷⁹¹, which would be applicable for knowledge retention too, but the reason for doing so was not specifically framed as a knowledge security concern. There was no direct mention of academic activity related to the concepts of ‘Knowledge Security’ or ‘Secure Knowledge Sharing’.

University of Washington – For the terms ‘Secure Knowledge Management’ and ‘Knowledge Protection’, no direct evidence was found relating to teaching and academic programs specifically linking knowledge and security. As with other universities, there was reference to issues around IP law⁷⁹². There was also some reference made to IP and security in the communication leadership curriculum relating to law and policy⁷⁹³. When searching for the term ‘Knowledge Security’, there was no current evidence found with regards to a teaching or academic focus around the topic. There was some mention of the topic in research and news articles still present on the university’s website, but this mostly related to the work of

⁷⁸⁸ University of North Carolina, 2012. *School of Information and Library Science: SILS Alumna, Meredith R. Evans Raiford Appointed Associate University Librarian* [Online].

⁷⁸⁹ University of North Carolina, 2017. *School of Information and Library Science: Brewster Kahle: "Universal Access to All Knowledge"* [Online].

⁷⁹⁰ University of North Carolina, 2011. *School of Information and Library Science: Connecting Clinical Informatics and Cancer Outcomes Research* [Online].

⁷⁹¹ University of North Carolina, 2015. *School of Information and Library Science: Special Course Topic Archive* [Online].

⁷⁹² University of Washington, 2020. *School of Law: Intellectual Property LL.M* [Online].

⁷⁹³ University of Washington, 2020. *My Plan: COMMLD 558 Law and Policy (5)* [Online].

Desouza⁷⁹⁴ while he was an academic at the university's information school, the majority being from the 2006-2007 period. After he left the university, it seems that this branch of research did not continue in any formal sense.

For the term 'Knowledge Loss', there was no direct reference found in the teaching curriculum. There was some indicative indirect engagement with the topic from a research perspective in the form of a 2014 student Capstone Project by Leung⁷⁹⁵, which dealt with the loss of experience and institutional knowledge in the University of Washington's library system due to employee retirement. While not a direct reference in teaching, it indicates some informal engagement around the topic, either as an element mentioned in class or through the interest of an academic advisor. There was also no direct mention of teaching or research related to the concepts of 'Knowledge Retention' or 'Secure Knowledge Sharing'.

Having completed the overview of findings for the USA universities, I will now discuss the findings in terms of the representation of knowledge concerning security as per the analysis of each of the targeted EUR universities. I will again outline those elements relating to a relationship found in teaching and academic programs where applicable.

5.3.2 EUR Universities Results and Findings

University of Sheffield – When searching for the term 'Knowledge Protection', as with other universities from the previous section, there was no direct evidence found other than results relating to IP protection from a legal standpoint in the fields of law⁷⁹⁶, engineering⁷⁹⁷ and international business development⁷⁹⁸. This is mostly related to things like data protection in the case of engineering, patents, trade secrets, trademarks and so forth as outlined in previous iterations of similar courses⁷⁹⁹. For the term 'Knowledge Retention', as with previous

⁷⁹⁴ Examples of references to Desouza's research interests in relation to knowledge security can still be found on the university website relating back to the 2006-2007 period, for example: <http://www.washington.edu/alumni/partnerships/ischool/200703/desouza.html>; <https://www.washington.edu/news/2007/05/31/kevin-desouza-small-office-big-impact/>; <https://www.washington.edu/news/2007/03/01/forum-looks-at-threat-of-cyber-terrorism/>

⁷⁹⁵ Leung, 2014. *Information School Capstone Research Poster - Forecasting the Future of Library Leadership at the UW Libraries* [Online].

⁷⁹⁶ The University of Sheffield, 2020. *Undergraduate Prospectus Law LLB - Property Law (Land Law, Equity and Trusts)* [Online].

⁷⁹⁷ The University of Sheffield, 2019. *General Engineering - MGT388 Finance and Law for Engineers* [Online].

⁷⁹⁸ The University of Sheffield, 2020. *Programme Regulations Finder, Departments & Services - MGT376 International Business* [Online].

⁷⁹⁹ The University of Sheffield, 2015. *Programme Regulations Finder, Departments & Services - LAW3020 Intellectual Property: Patents, Trade Secrets* [Online].

universities, from an HR perspective, there were some course references relating to the importance of staff retention⁸⁰⁰, which would be applicable for knowledge too, but the reason for doing so was not specifically framed as a knowledge security concern. There was no direct mention of teaching or research related to the concepts of ‘Secure Knowledge Management’, ‘Knowledge Security’, ‘Knowledge Loss’, ‘Knowledge Retention’ or ‘Secure Knowledge Sharing’.

Tampere University – For the term ‘Knowledge Protection’, while there was no confirmable evidence of teaching taking place in this regard, as the university website was not clear on this, there was solid evidence of research being done into knowledge protection by some members of staff. Under the profile of university instructor Ilona Ilvonen, whose research was mentioned in the literature review done in Chapter 4, they list knowledge protection as one of their research interests⁸⁰¹. In one of their previous research papers, they outlined a study that they had done related to the state of knowledge protection in Finnish companies of different sizes⁸⁰² confirming their research interest. There was no direct mention of teaching or research related to the search terms of ‘Secure Knowledge Management’, ‘Knowledge Security’, ‘Knowledge Loss’ or ‘Secure Knowledge Sharing’.

University of Borås – Concerning the information available on the university website, not much could be found. For the term ‘Knowledge Security’, no direct evidence was found, with only some partial legacy evidence of interest in the topic from 2011, relating to a workshop with the focus on the web of the future. In the workshop presentation document, there was some mention of digital preservation when talking about the Sustaining Heritage Access Through Multivalent Archiving (SHAMAN) European Union project related to information and knowledge⁸⁰³. This was not specifically linked in terms of a connection between knowledge and security issues. There was also no direct mention of teaching or research related to the search terms of ‘Secure Knowledge Management’, ‘Knowledge Protection’, ‘Knowledge Loss’, ‘Knowledge Retention’ or ‘Secure Knowledge Sharing’.

⁸⁰⁰ The University of Sheffield, 2020. *Sheffield University Management School - Management School, MSc Human Resource Management with CIPD Pathway modules* [Online].

⁸⁰¹ Tampere University, 2020. *Profile, Ilona Ilvonen: University Instructor, Information and Knowledge Management* [Online].

⁸⁰² Ilvonen, *et al.*, 2016. *Knowledge Sharing and Knowledge Security in Finnish Companies* p 4021-4030.

⁸⁰³ Darányi, 2011. *Discussion Workshop - The SHAMAN EU Project in a Nutshell: What next?* University of Borås [Online].

University of Amsterdam – For the term ‘Knowledge Protection’, while no direct evidence could be found, there appears to be some indirect legacy evidence related to teaching in this regard. In 2016, there was a short course in entrepreneurship for master’s students⁸⁰⁴. One of the topics listed to be covered in the course was IP and knowledge protection. While it is not clear as to the contents of the topics, as the course details are no longer available, this likely meant dealing with things like patents, copyright, trademarks etc., based on what other universities have done in this regard. What is interesting is that they linked the concepts of IP and knowledge protection directly.

For the term ‘Knowledge Retention’, while no direct evidence was found concerning teaching and academia, some postgraduate research indirectly dealt with knowledge retention issues. This was in the form of a doctoral dissertation done by Kuvik in 2015. Kuvik⁸⁰⁵ examined the global competition for talent and framed the issue from the perspective of ensuring that groups of people remain in a country so their knowledge would not be lost. The idea is that by implementing measures to retain people and their knowledge, the country could stay competitive and compete in the global knowledge economy. There was no direct mention of teaching or research related to the search terms of ‘Secure Knowledge Management’, ‘Knowledge Security’, ‘Knowledge Loss’, ‘Knowledge Retention’ or ‘Secure Knowledge Sharing’.

Loughborough University – For the term ‘Knowledge Protection’, while no direct evidence was found concerning teaching, within the university system there was some mention of legacy research into issues related to IP protection from an economics driven perspective, concerning patents⁸⁰⁶. However, nothing was specifically mentioned in terms of IP protection as a mechanism of knowledge protection. For the term ‘Knowledge Retention’, there was a recent mention in the *School of Business and Economics Inspire Magazine* when discussing the Centre for Corporate Entrepreneurship and Innovation⁸⁰⁷. This took the form of mentioning that a lack of knowledge retention in organisations can inhibit an organisation’s ability to innovate and stay competitive, but this was very minimal and did not go into any detail. Apart from this, there was no direct mention of teaching or research related to the search terms of ‘Secure

⁸⁰⁴ University of Amsterdam, 2016. *2-day Course in Entrepreneurship for Master’s Students (2 ECTS Credits): How to Successfully Start a Company or New Venture* [Online].

⁸⁰⁵ Kuvik, 2015. *Summary: The Global Competition for Talent: Life Science and Biotech Careers, International Mobility, and Competitiveness*.

⁸⁰⁶ Mukherjee, 2014. *Patent Protection Under Endogenous Product Differentiation* p 80-83.

⁸⁰⁷ Hughes, 2020. *Introducing the Centre for Corporate Entrepreneurship and Innovation* [Online].

Knowledge Management’, ‘Knowledge Security’, ‘Knowledge Loss’ or ‘Secure Knowledge Sharing’.

5.4 Discussion of Findings

In the section to follow, I will discuss these findings and how they relate to my initial assumption, as well as provide a brief discussion on the limitations of the research. Concerning my general observations of the findings for each of the universities analysed, it seems that any activities which could be related to the security of knowledge are largely based around the concepts of IP protection, staff retention and information security activities. There also appeared to be some minimal research interest into the topic at a staff level and postgraduate level, but not always directly. Each of which will be discussed in more detail. I will also discuss my final thoughts as to how this relates to my initial assumptions of a link between knowledge and security in academia, as well as the limitations of this chapter’s analysis.

5.4.1 General Observations of the Findings

Firstly, in terms of IP, this appears to be framed from a legal, IT systems, leadership, international business development, economic or engineering standpoint. Ultimately, the different flavours of these approaches mentioned all boil down to the implementation of legal mechanisms to secure the proprietary knowledge of an organisation. This is done through mechanisms like patents, copyrights, non-disclosure agreements (NDAs) and so forth. Generally, apart from the University of Amsterdam, there was no attempt to make a direct link between knowledge protection and IP in other listed universities’ teaching and academic materials. Ultimately, whether mentioned or not, they all relate back to the same general legal concepts and mechanisms.

Secondly, in terms of the retention of people, which could be construed as a mechanism of knowledge protection from a KM perspective too, there was some mention of this. It was generally framed from a knowledge governance or HR perspective to retain key individuals, and by proxy their knowledge and skills, to remain innovative and competitive. There was some mention too, from a postgraduate research perspective, related to preventing knowledge loss due to staff retiring and how to mitigate its impact. Additionally, this was mentioned from an archival process and systems perspective. Some postgraduate research also mentioned the importance of retaining workers and their knowledge, to allow a country to remain innovative and thus competitive in the global knowledge economy. This, however, was generally not a

common view, although it was mentioned in Chapter 4, when conducting the literature review pertaining to the retention of individuals with nuclear industry knowledge.

Thirdly, in terms of linking the topic to information security issues, there appeared to be some minimal attempts of doing this, but from the perspective of teaching both KM and IM together and linking them in that way. However, any security mechanisms given were discussed from an information security perspective and not a knowledge security perspective. This would relate to things like information systems and could be conceived of applying to things like KMSs too. While there was some mention of security being important for KM, it was not specifically focused on KM and security, but rather appeared to be generally linked to the objectives of organisational information governance.

Fourthly, from a research perspective, there was some minimal evidence found relating to issues of knowledge and security, but this was not at a substantial level across the board. It appeared that any departmental research into topics linking knowledge and security were largely driven by the research interests of certain academics and any research groupings they may have belonged to. Some indirect indication of interest in the topic was also observed through the research topics of a few postgraduate students in the respective universities analysed. For example, at Tampere University, there appears to be some current interest and research into the topic of knowledge protection, but it appears to be mostly driven by the research interests of a single person or small research group. At some universities, it seems that there was an interest in the security of knowledge in the past, based on previous legacy research conducted, but this appears to relate more to the interests of key champions of the topic. Once these champions left, the research tapered off and was no longer as popular. Concerning postgraduate research into the topic, some dissertations referred to aspects of the idea of the security of knowledge, as a contributor to organisational performance; a similar position taken by some authors mentioned in the literature review as discussed in Chapter 4. Thus, based on these findings, it appears that while there seems to be some interest in the topic, its success is largely driven by key individuals who champion the concept in their respective universities. Once they move on, it appears that in most cases so does that departments interest in the topic too.

5.4.2 Validity of Original Assumptions Made

My original assumption was that I would not find much evidence linking knowledge to security in leading universities' teaching and academic programs. Concerning how these findings relate

to my original assumption, there was perhaps more interest in the topic than I was initially expecting, but overall, it was still quite minimal and certainly not mainstream in most instances. This relates to the legal and HR focus as well as information security and knowledge governance issues mentioned. Thus, I would make the conclusion that even though there are pockets of interest in the topic, or where there are other fields that cover issues related to the topic, it is not generally taught as a formal course across the universities investigated. This is not to say that it is not taught at all in any other academic programs at different universities. For example, a masters level course in KM and security was mentioned by Padyab *et al.* as part of their research into the genre-based approach to assessing information and knowledge security risks⁸⁰⁸. But rather, that it is not taught as a formal course at those universities perceived to be at the forefront of research in the field of information science and studies.

In terms of this finding being translated into practice, I would thus also expect there to be a focus on issues surrounding IP, HR retention issues, some general knowledge archiving and transfer and some focus on information security as a mechanism that can also be used to secure KMSs from a knowledge governance perspective. Beyond that, I do not expect there to be much more of a development in terms of linking KM with security within organisations and their relevant functions. This assumption will be analysed and tested in Chapter 6, relating to the completion of my interview process with relevant employees of companies perceived to be leaders in the field of KM.

5.4.3 Limitations of the Research and Analysis

Finally, while I did do as much as possible to mitigate the effects of any research limitations within the scope of my research objective, it is important to note that there are still some factors to be aware of. Firstly, the sample size examined is small and is not representative of the knowledge security teaching activities taking place in all universities. As initially stated, this was justified as the objective was to examine what is happening at the top level of academic teaching to see where leading universities in the field are focusing their attention. Additionally, when looking at the quantity of the literature available, as discussed in Chapter 5's literature review, there appears to be a much smaller body of knowledge available. This to me would indicate that there is less research being done with regards to this topic at other universities too.

⁸⁰⁸ Padyab *et al.*, 2014. *Genre-Based Approach to Assessing Information and Knowledge Security Risks* p 20.

Secondly, there is also the risk that I might have missed some information relating to teaching or research activities at these leading universities, as it is not always possible to examine the finer details of courses or general mentions of the topic on their websites. In their teaching activities related to KM, there is the possibility that some departments at the universities examined may have included some information related to knowledge and security in their course work but did not list it as a separate area of study, rather being placed under the broader KM course headline or module. Additionally, there might also be some information that is not publicly accessible but that would be accessible through a university portal and as such I would not be able to access this material for further analysis. This could therefore potentially limit the depth of some of my results to a small degree, by only being able to focus on what is open and accessible.

Thirdly, as certain universities are in countries whose primary language is not English, some documents or website entries related to what is being taught or researched within their respective departments may have been missed as my searches were conducted in English. As stated earlier in this chapter, I did aim to choose those universities that also offered an English version of their respective websites to mitigate this risk. However, there is still a possibility that I failed to find some material that was not in English, but in the primary language of the institution; potentially limiting my scope to a small degree once again.

5.5 Conclusion

Chapter 5 formed the first part of the empirical analysis and aimed at examining if knowledge and security are treated as separate entities in the teaching and academic programs at leading universities. This was in line with the research question as illustrated in Chapter 1, Figure 1-2⁸⁰⁹. To achieve this aim, Chapter 5 followed an open-access approach. The approach consisted of a review of the leading universities' websites to establish whether knowledge and security are treated as separate entities in their teaching and academic programs. The approach was premised on the view that what is taught at leading universities in the field will provide a representation of what the state of the art is and thus what is likely being followed by organisations too. The chapter began by firstly outlining the process of identifying the leading universities. Next, the universities websites were examined in greater detail using advanced search parameters to establish if such a relationship exists. The findings of the analyses were

⁸⁰⁹ Research sub-question 5.1: *Are knowledge and security treated as separate entities in teaching and academic programs at leading universities?*

outlined for each university in turn for the regions under investigation. Finally, the findings were discussed, and observations from the findings were drawn. With this analysis acting as the theoretical foundation of the state of the art, the examination of what is being done in practice, with regards to KM and security, will be discussed in Chapter 6 to follow. This will form the second part of the empirical analysis and pertains to the research objectives of establishing if what is done in practice reflects those elements found in academic teaching and what the relationship between KM and security is in practice.

Chapter 6

Review of Knowledge Security in Practice

6.1 Introduction

This chapter forms the second part of the empirical component. It outlines the research process and findings related to determining if what is done in practice reflects the elements found in academic teaching as discussed in Chapter 5. It also helps in obtaining a practical perspective of KM and its relationship with security. The objective of this is to inform Chapter 7's discussion concerning the conceptual model inputs. To achieve these objectives, a qualitative, interpretive research approach was used⁸¹⁰. Practically, this consisted of a series of semi-structured interviews with industry experts, resulting in the output of several case study narratives. The research process and the findings are discussed in more detail in the sections to follow. These are structured around the research design, research method, analysis, and findings.

6.2 Research Design

For the final part of the empirical analysis, I examined what is being done in practice by those considered to be experts in the use and application of KM. I did this to fulfil the research objectives of garnering a practical insight into KM and security and to determine the alignment of academic teaching with knowledge security issues. It should be noted that unlike larger academic studies where the empirical research forms the entire project, this aspect is but one component of my broader research. The primary objective here is to examine the relationship between those elements mentioned in academic teaching relating to knowledge security. It is also to garner a practical understanding and input for the discussion of the conceptual model. Thus, it is not the sole focus of the project, and as such was dealt with in a slightly less in-depth

⁸¹⁰ Ponelis, 2015. *Using Interpretive Qualitative Case Studies for Exploratory Research in Doctoral Studies: A Case of Information Systems Research in Small and Medium Enterprises* p 535-550.

way than would be if it were the entire basis of the research. However, it is still appropriate to the outcomes and objectives of the broader project and was therefore felt to adequately meet these needs in context. My approach to this has been adapted from the research approach outlined by Ponelis⁸¹¹ related to using interpretive qualitative case studies in information systems research. As such, I have used those relevant elements mentioned by Ponelis as a guide to structuring this phase of the research presented in this chapter. In the sections to follow, the components of the research design are discussed in more detail. These consist of discussions around the research paradigm, case-based research, the unit of analysis used and the selection of cases.

6.2.1 Research Paradigm

When conceptualising this part of the research, it was suggested that I conduct a series of qualitative interviews to obtain a practical understanding of KM and security. However, as the selected research design is dependent on the chosen research paradigm⁸¹², I first needed to examine in more detail how to approach my analysis. Two of the most common views used in information studies and systems are the interpretivist and positivist paradigms⁸¹³, framed within the qualitative methodological base⁸¹⁴.

Firstly, concerning the interpretivist paradigm, Coffey and Atkinson⁸¹⁵ state, as mentioned by Ponelis⁸¹⁶, that “knowledge generation happens when relevant insights emerge naturally through researcher-participant discourse”. In essence, this means that our knowledge of reality is a social construct, based on perception⁸¹⁷, occurring from the interaction between human actors within their environment⁸¹⁸. Thus, the assumption here is that the researcher’s view will be centred within the findings of a study because meaning is constructed through this

⁸¹¹ Ponelis, 2015. *Using Interpretive Qualitative Case Studies for Exploratory Research in Doctoral Studies: A Case of Information Systems Research in Small and Medium Enterprises* p 535-550.

⁸¹² Creswell, 2009. *Research design: Qualitative, Quantitative, and Mixed Methods Approaches*.

⁸¹³ Leitch *et al.*, 2010. *The Philosophy and Practice of Interpretivist Research in Entrepreneurship: Quality, Validation, and Trust* p 67-84.

⁸¹⁴ Mason, 2002. *Designing Qualitative Research* p 2.

⁸¹⁵ Coffey & Atkinson, 1996. *Making Sense of Qualitative Data*.

⁸¹⁶ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 70.

⁸¹⁷ Cavana *et al.*, 2001. *Applied Business Research: Qualitative and Quantitative Methods*.

⁸¹⁸ Burrell & Morgan, 2017. *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*.

interaction⁸¹⁹. While this can create a perceived risk of bias, the interpretivist paradigm assumes that a study can never be bias-free and eliminating bias would not be a research intention⁸²⁰. Myers explains that access to reality is attainable only through the social constructs of language and shared meaning⁸²¹. The objective of interpretive research is thus to understand rather than predict⁸²², where variables are not predefined⁸²³. Rather the researcher plays an active role in that they would attend to how their thoughts, feelings, opinions, and experiences might influence what they record in terms of jointly constructing knowledge⁸²⁴.

Secondly, concerning the positivist paradigm, Ponelis⁸²⁵ states that it is “based on a realist ontology that assumes observation is theory-neutral and the role of scientific research is to make generalisations to account for what was observed”. From the positivist view, emphasis is placed on overarching patterns of human behaviour, with little value seen in capturing in-depth information about the experiences of individuals⁸²⁶. Rather, the effects of an intervention would be examined, either quantitatively or qualitatively⁸²⁷, within the positivist paradigm⁸²⁸. Bunniss and Kelly⁸²⁹ further discuss that from a positivist paradigm; data collection in naturalistic settings would be avoided as it introduces further variables. Instead, the focus would be on measuring “predetermined characteristics of a particular phenomenon”⁸³⁰, thus eliminating the need to be responsive to participants in the same way during data collection.

All of these characteristics of data gathering reflect the ontological assumption that reality exists objectively and the epistemological assumption that it can be most accurately described using deductive reasoning. These design characteristics reflect

⁸¹⁹ Weaver & Olson, 2006. *Understanding Paradigms Used for Nursing Research* p 459-469.

⁸²⁰ Bunniss & Kelly, 2010. *Research Paradigms in Medical Education Research* p 358-366.

⁸²¹ Myers, 2009. *Qualitative Research in Business and Management*.

⁸²² Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 70.

⁸²³ Kaplan & Maxwell, 2005. *Qualitative Research Methods for Evaluating Computer Information Systems* p 30-55.

⁸²⁴ Bunniss & Kelly, 2010. *Research Paradigms in Medical Education Research* p 358-366.

⁸²⁵ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 70.

⁸²⁶ Bunniss & Kelly, 2010. *Research Paradigms in Medical Education Research* p 358-366.

⁸²⁷ Park *et al.*, 2020. *The Positivist Paradigm of Research* p 690-694.

⁸²⁸ Chua *et al.*, 2019. *Capturing the Patient Voice Through Patient Experience Debriefs: How Medical Student-Led Debrief Interviews of Hospitalized Families Influence Learning and Reflection* p 86-94.

⁸²⁹ Bunniss & Kelly, 2010. *Research Paradigms in Medical Education Research* p 358-366.

⁸³⁰ Bunniss & Kelly, 2010. *Research Paradigms in Medical Education Research* p 358-366.

the ontological and epistemological assumptions that are particular hallmarks of the positivist paradigm⁸³¹.

In light of this and given the context I am examining, I chose to follow a qualitative interpretivist paradigm, as is commonly used in information studies⁸³² and systems research⁸³³. While some authors⁸³⁴ view the interpretive paradigm as a minority position, its use still holds merit in certain cases such as this one, where the qualitative interpretivist view is particularly applicable when trying to gain an understanding of something in context⁸³⁵. Al-Busaidi⁸³⁶ points out that under the umbrella of qualitative research, interpretative techniques seek to describe, decode, translate, and come to terms with the meaning, not frequency, of naturally occurring phenomena in the social world. According to Bygrave⁸³⁷, using the interpretive approach enables the researcher to yield a richer understanding of the key issues being examined, particularly in organisational contexts. The reason for this is that it allows for a more flexible analysis based on linguistic meaning and understanding, where a numerical analysis would be less appropriate⁸³⁸. Therefore, as my objective is to better understand KM in practice and its relationship with security from an expert's view, it was deemed most appropriate.

6.2.2 Case-Based Research

With the qualitative interpretivist paradigm in mind, I selected to make use of a qualitative case-based research methodology. According to Perry *et al.*⁸³⁹, as cited in Ponelis⁸⁴⁰, case-based research is an appropriate methodology used to answer research questions within the interpretivist paradigm and is one that can be applied to a range of topics and purposes⁸⁴¹.

⁸³¹ Bunniss & Kelly, 2010. *Research Paradigms in Medical Education Research* p 358-366.

⁸³² Kankam, 2019. *The Use of Paradigms in Information Research* p 85-92.

⁸³³ Goldkuhl, 2012. *Pragmatism vs Interpretivism in Qualitative Information Systems Research* p 135-146.

⁸³⁴ Bevir & Kedar, 2008. *Concept Formation in Political Science: An Anti-Naturalist Critique of Qualitative Methodology* p 503-517.

⁸³⁵ Kankam, 2019. *The Use of Paradigms in Information Research* p 85-92.

⁸³⁶ Al-Busaidi, 2008. *Qualitative Research and its Uses in Health Care* p 11-19.

⁸³⁷ Bygrave, 1989. *The Entrepreneurship Paradigm (I): A Philosophical Look at its Research Methodologies - Entrepreneurship Theory and Practice* p 7-26.

⁸³⁸ Elliott & Timulak, 2005. *Descriptive and Interpretive Approaches to Qualitative Research: A Handbook of Research Methods for Clinical and Health Psychology* p 147.

⁸³⁹ Perry *et al.*, 1999. *Realism's Role Among Scientific Paradigms in Marketing Research* p 16-23.

⁸⁴⁰ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 75.

⁸⁴¹ Stewart cited in Jane Mills & Melanie Birks (Eds.), 2014. *Qualitative Methodology: A Practical Guide* p 145-159.

Harrison *et al.*⁸⁴² suggest that the essential requisite for employing a case study approach stems from the motivation to illuminate understanding of complex phenomena. They proceed to explain that case studies are primarily exploratory and explanatory and are used to gain an understanding of the issue in real-life settings. Ponelis states that “when seeking understanding, as in exploratory research, case studies are the most appropriate method”⁸⁴³ to use. Case studies also have the benefit of increasing the relevance of research, due to their ability to illuminate practice in ways that surveys or laboratory experiments cannot⁸⁴⁴.

6.2.3 Unit of Analysis

To garner a broad level understanding of KM in practice, and any relationship to security issues, required the views of experienced experts within leading organisations where possible, on an individual level. This view is validated by Rowley⁸⁴⁵, as cited in Ponelis⁸⁴⁶, who explains that the unit of analysis, amongst others, can be an individual who has experience or interest for the study or an organisation or part thereof. Similar studies in KM have been done using multi-case analysis, such as that by Cranfield and Taylor⁸⁴⁷, where the unit of analysis was a series of organisations and where interviews were conducted with identified knowledgeable participants in the selected organisations. Hence, the relevant experienced individual within the appropriate organisations, where possible, is the primary unit of analysis in this investigation.

It should be noted that the initial approach proposed was to investigate a group of key individuals within two leading KM orientated companies. However, in practice, this was found not to be possible due to a lack of access to key individuals within the same organisations. It was therefore decided to extend the study to include those experts referenced by participants outside of the initial scope of the two leading organisations, but who was still ranked by their peers as experts in the field. Newington and Metcalfe state that when it comes to overcoming recruitment issues, “strategies need to be relevant to the target population and the research

⁸⁴² Harrison *et al.*, 2017. *Case Study Research: Foundations and Methodological Orientations*.

⁸⁴³ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 70.

⁸⁴⁴ Arnott & Pervan, 2005. *A Critical Analysis of Decision Support Systems Research* p 67-87.

⁸⁴⁵ Rowley, 2002. *Using Case Studies in Research* p 16-27.

⁸⁴⁶ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 77.

⁸⁴⁷ Cranfield & Taylor, 2008. *Knowledge Management and Higher Education: A UK Case Study* p 85-100.

methodology used, and therefore the optimum strategy is likely to vary”⁸⁴⁸. The approach taken in this instance was still deemed justifiable after consultation with academics and business professionals on how to overcome the issue and was taken in the light of their suggestions⁸⁴⁹. Further, it was not deemed to compromise the integrity of the investigation greatly, since the research is focused on gaining understanding from experts and was still deemed to be relevant to the methodological framework and target group of the study.

6.2.4 Selection of Cases

The initial approach to the selection of cases aimed to make selections from a pool of award-winning KM organisations. These were to be based on the current list of winners of the Most Admired Knowledge Enterprise (MAKE) awards, a globally recognised KM award⁸⁵⁰. Unfortunately, since the time of writing my initial research proposal, the MAKE awards have ended⁸⁵¹, with the last year of global winners available for 2017⁸⁵². In 2018, a new award was launched called the Most Innovative Knowledge Enterprise (MIKE) awards. This award is structured on the original MAKE framework⁸⁵³ but with an updated focus and body responsible for administering it. While it would make sense to substitute the MAKE for the MIKE winners in my selection, the MIKE awards are still relatively new and still in the process of expanding to be globally inclusive⁸⁵⁴. Currently, the MIKE awards are focused on regional representation, with each iteration of the award being expanded to be more globally representative. The objective of the MIKE awards is to eventually identify the top 100 best KM global winners in 2020⁸⁵⁵, but at the time of writing has not currently been released. In terms of my research objectives, this creates a situation where the older MAKE awards are globally representative, but not as up to date. Similarly, where the MIKE awards are up to date, but not as globally representative.

⁸⁴⁸ Newington & Metcalfe, 2014. *Factors Influencing Recruitment to Research: Qualitative Study of the Experiences and Perceptions of Research Teams* p 10.

⁸⁴⁹ This was done through an anonymous brainstorming session using the Crealogic collaboration software.

⁸⁵⁰ The Hong Kong Polytechnic University & Arup University, 2020. *Knowledge Management and Innovation Research Centre: Hong Kong MIKE Award 2020 Briefing Session* [Online].

⁸⁵¹ The Hong Kong Polytechnic University & Arup University, 2020. *Knowledge Management and Innovation Research Centre: Hong Kong MIKE Award 2020 Briefing Session* [Online].

⁸⁵² Most Innovative Knowledge Enterprise, 2020. *About Us* [Online].

⁸⁵³ Most Innovative Knowledge Enterprise, 2020. *About Us* [Online].

⁸⁵⁴ The Hong Kong Polytechnic University & Arup University, 2020. *Knowledge Management and Innovation Research Centre: Hong Kong MIKE Award 2020 Briefing Session* [Online].

⁸⁵⁵ The Hong Kong Polytechnic University & Arup University, 2020. *Knowledge Management and Innovation Research Centre: Hong Kong MIKE Award 2020 Briefing Session* [Online].

To overcome this issue, I approached the selection of organisations by integrating the two lists through a process of aggregation and filtering. I did so to build a more comprehensive representation of organisations likely to be consistently recognised for their KM efforts. This was modelled on the process followed in Chapter 5 when selecting relevant universities to examine. For this integration, I chose to include the MAKE winners lists from 2015-2017, to keep the inclusion as recently representative as possible. For the MIKE winners, I selected the currently available lists from 2018-2019, to keep the inclusion of organisations as recently applicable as possible. The identified MAKE and MIKE winners for the respective years are listed in Tables 6-10 and 6-11. These consist of the awarding body, the region covered, the year of the award, and the list of winning organisations for the respective year.

Having compiled the list, I proceeded with the aggregation process using “Conditional Formatting” and the “COUNTA” function in my spreadsheet software to group and count the KM winners. Each time an organisation appeared on a list, I awarded them one point. For the MIKE awards lists, where the same company appeared multiple times for different regions, as with EY, I consolidated these entries and assigned the single company with the relevant points. When prioritising companies to contact, I proceeded to filter the remaining companies, as shown in Table 6-12, according to two criteria: 1) Organisations with a point score ≥ 2 awarded points. 2) Organisations that had local representation (represented by “L” in Table 6-12).

For criterion one, having two or more points as a filter was considered important, as those organisations that won multiple times are likely to be more representative of consistency in KM and thus performance when it comes to the extenuation of their KM efforts. For criterion two, I gave preference to companies with local representation to ease the barrier of access to relevant people within the chosen organisations. I based this on the assumption that they would be more familiar with my university, academic department or possibly know people in my academic or business network and would thus be more open to engaging with me. Guillermin *et al.*⁸⁵⁶ point out that when it comes to case study research, participants indicated that familiarity with the researcher’s university played a pivotal role in their willingness to participate. It was assumed by research participants that the university played a role as a guarantor for the research and that the researcher would be governed by the institution’s

⁸⁵⁶ Guillermin *et al.*, 2018. *Do Research Participants Trust Researchers or Their Institution?* p 285-294.

research ethics regulations⁸⁵⁷. Thus, local familiarity with my institution was considered as a trust factor when selecting participants for the study.

Table 6-10: List of Identified MAKE 2015-2017

Region	Year	Winners List	
Most Admired Knowledge Enterprise (MAKE)			
Global (All Regions) ⁸⁵⁸	2015	<ul style="list-style-type: none">• Accenture• Apple• BMW• ConocoPhillips• EY• Facebook• Fluor• FMC Technologies• Google• IBM• Infosys Limited	<ul style="list-style-type: none">• Microsoft• Phillips 66• PwC• Samsung• Schlumberger• Siemens• Tata Group• Tesla Motors• Wipro Limited
Global (All Regions) ⁸⁵⁹	2016	<ul style="list-style-type: none">• Accenture• Alphabet• Amazon.com• Apple• ConocoPhillips• Deloitte• Ecopetrol• EY• Fluor• FMC Technologies• IBM	<ul style="list-style-type: none">• Infosys Limited• Microsoft• PwC• Samsung Group• Schlumberger• Siemens• Tata Group• Tesla Motors• Wipro Limited
Global (All Regions) ⁸⁶⁰	2017	<ul style="list-style-type: none">• Accenture• Alphabet• Amazon.com• Apple• ConocoPhillips• Deloitte• EY• Facebook• General Electric• IBM• Inditex	<ul style="list-style-type: none">• LEGO• McKinsey & Company• Microsoft• PwC• Samsung Group• Schlumberger• Siemens• Tata Group• Wipro Limited

⁸⁵⁷ Guillemin *et al.*, 2018. *Do Research Participants Trust Researchers or Their Institution?* p 285-294.

⁸⁵⁸ Teleos, 2015. *2015 Global Most Admired Knowledge Enterprises (MAKE) Report* p 1-14.

⁸⁵⁹ Teleos, 2016. *2016 Global Most Admired Knowledge Enterprises (MAKE) Report* p 1-14.

⁸⁶⁰ Teleos, 2017. *2017 Global Most Admired Knowledge Enterprises (MAKE) Report* p 1-15.

Table 6-11: List of Identified MIKE Winners 2018-2019

Region	Year	Winners List	
Most Innovative Knowledge Enterprise (MIKE)			
Asian/Regional (Asia including Australia and New Zealand) ⁸⁶¹	2018	<ul style="list-style-type: none">• Afcons Infrastructure Limited• BINUS University• China Petroleum & Chemical Corporation (Sinopec Corp)• China Southwest Architectural Design and Research Institute Corp., Ltd• CinnaGen Company• CLP Power HK Ltd• EY, Australia & New Zealand• EY, Hong Kong• Faculty of Sciences, Saint-Joseph University of Beirut, Lebanon	<ul style="list-style-type: none">• Hong Kong Correctional Services Department• Hong Kong Police Force• Infosys Limited• Mindtree Ltd• NetEase Games• Sansan, Inc.• Wipro Limited
Asian/Global (Asia including the Middle East/North Africa) ⁸⁶²	2019	<ul style="list-style-type: none">• Afcons Infrastructure Limited• Architectural Services Department• BINUS University, Indonesia• China Asset Management Co., Ltd• China Petroleum & Chemical Corporation (Sinopec Corp)• China Southwest Architectural Design and Research Institute Corp., Ltd• CinnaGen Company• CLP Power Hong Kong Limited• Cognizant Technology Solutions• EY• Far East Holding Group Co., Ltd.	<ul style="list-style-type: none">• Fung Academy• Hong Kong Correctional Services Department• Infosys Limited• Mobarakeh Steel Company (MSC)• NetEase Games (Guangzhou Boguan Information Technology Co., Ltd)• NKE Corporation• Petroleum Development Oman LLC• Sino Innovation Laboratory Limited• Tata Chemicals• Think&Act,Inc.• Wipro Limited

⁸⁶¹ Global MIKE Study Group, 2018. *MIKE Award: Winners of the Asian Global MIKE Award 2018 (in Alphabetical Order)* [Online].

⁸⁶² Global MIKE Study Group, 2019. *MIKE Award: Winners of the Global MIKE Award 2019 (in Alphabetical Order)* [Online].

Table 6-12: Consolidated List of Identified MIKE and MAKE Organisations

Consolidated Winners List			
• EY	5 (L)	• Hong Kong Correctional Servi...	2
• Wipro Limited	5 (L)	• NetEase Games (Guangzhou B...	2
• Tata Group	4 (L)	-----	
• Accenture	3 (L)		
• Apple	3	• BMW	1
• ConocoPhillips	3	• Ecopetrol	1
• IBM	3 (L)	• Google	1
• Infosys Limited	3 (L)	• General Electric	1
• Microsoft	3 (L)	• Inditex	1
• PwC	3 (L)	• LEGO	1
• Samsung	3 (L)	• McKinsey & Company	1
• Schlumberger	3 (L)	• Phillips 66	1
• Siemens	3 (L)	• Architectural Services Depart...	1
• Alphabet	2	• China Asset Management Co...	1
• Amazon.com	2 (L)	• Cognizant Technology Soluti...	1
• Deloitte	2 (L)	• Faculty of Sciences, Saint-Jo...	1
• Facebook	2 (L)	• Far East Holding Group Co. ...	1
• Fluor	2 (L)	• Fung Academy	1
• FMC Technologies	2	• Infosys Limited	1
• Tesla Motors	2	• Mobarakeh Steel Company (MSC)	1
• Afcons Infrastructure Limited	2	• NKE Corporation	1
• BINUS University, Indonesia	2	• Petroleum Development Om...	1
• China Petroleum & Chemical...	2	• Sino Innovation Laboratory...	1
• China Southwest Architecture...	2	• Hong Kong Police Force	1
• CinnaGen Company	2	• Think&Act, Inc.	1
		• Mindtree Ltd	1
		• Sansan, Inc.	1

Through this process, I shortlisted a group of 15 preferred KM orientated organisations to contact. The hope was that the required number of participants from 2 of the 15 organisations listed would agree to participate in line with the objectives of the research approach. The number of organisations identified is also in line with other similar types of studies done in the field of information science⁸⁶³. This means that while interviews would only be conducted at two organisations, a longer list was compiled to account for any non-replies, rejections, withdrawals, or organisations found not to meet my criteria after further evaluation. While there is no agreement as to how many cases a researcher should select⁸⁶⁴, there are still several recommendations made in the literature⁸⁶⁵.

⁸⁶³ Ponelis, 2015. *Using Interpretive Qualitative Case Studies for Exploratory Research in Doctoral Studies: A Case of Information Systems Research in Small and Medium Enterprises* p 535-550.

⁸⁶⁴ Vissak, 2010. *Recommendations for Using the Case Study Method in International Business Research* p 370-388.

⁸⁶⁵ Ponelis, 2015. *Using Interpretive Qualitative Case Studies for Exploratory Research in Doctoral Studies: A Case of Information Systems Research in Small and Medium Enterprises* p 535-550.

For example, Rowley⁸⁶⁶ suggests that a study of 6 to 10 cases works well, with Crabtree and Miller⁸⁶⁷ suggesting that a sample size of 6 to 8 subjects is best suited for homogeneous samples. Eisenhardt⁸⁶⁸ contends that a study of 4 to 10 cases works well while having less than four cases can make it more difficult to generate theory and having more than 10 cases can make the volume of data difficult to cope with. This view is also supported by Miles and Huberman⁸⁶⁹, who argue that selecting more than 15 cases can make a study unwieldy. Opposed to this view is Gummesson⁸⁷⁰, who states that almost any number of cases can be justified, even hundreds of cases. But as Vissak⁸⁷¹ states, “it can be questioned if it is reasonable to spend considerable time on making hundreds of case studies”, even if increasing the generalisability of the results, as the richness and depth of the results can be lost. Thus, defeating the purpose of using a case-based approach in the first place.

Based on these recommendations, I chose to interview 5 to 10 participants for my research. Concerning the profile of the participants, I aimed for knowledgeable individuals who had a minimum of five years’ experience. Five years was chosen as a cut-off point, as this was advised to me by an HR professional to be the minimum threshold to be considered as senior for a role⁸⁷². My initial approach to finding the participants, as suggested in the literature⁸⁷³, consisted of identifying contacts at the relevant organisations through my networks and word-of-mouth referrals⁸⁷⁴. I also tried contacting the organisations directly to see if there would be individuals willing to participate or to suggest who I might contact internally.

Once initial participants had been identified, I would find further participants using snowball exponential non-discriminative sampling⁸⁷⁵. Practically, this would mean asking existing participants for references to other relevant participants in their organisation. As I was not

⁸⁶⁶ Rowley, 2002. *Using Case Studies in Research* p 16-27.

⁸⁶⁷ Crabtree & Miller, 1992. *Doing Qualitative Research*.

⁸⁶⁸ Eisenhardt, 1989. *Building Theories from Case Study Research* p 532-550.

⁸⁶⁹ Miles & Huberman, 1994. *Qualitative Data Analysis: An Expanded Sourcebook*.

⁸⁷⁰ Gummesson, 2003. *All Research is Interpretive* p 482-492.

⁸⁷¹ Vissak, 2010. *Recommendations for Using the Case Study Method in International Business Research* p 370-388.

⁸⁷² Paulsen, Z. 2020. *Personal Interview*.

⁸⁷³ Hartley, 1994. *Case Studies in Organisational Research* p 208-229.

⁸⁷⁴ Chibelushi & Costello, 2009. *Challenges Facing W. Midlands ICT-Oriented SMEs* p 210-239.

⁸⁷⁵ Dudovskiy, 2016. *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance*.

dealing with a set of hard to pin down respondents⁸⁷⁶, the snowball technique was thought to be a valid form of investigation in this instance. Bias in the selection of respondents, and as such the results, would be reduced as I was targeting organisations and respondents with defined boundaries and allocated positions. As this is in line with general research principles in business studies⁸⁷⁷, it was decided that following a similar approach would allow me to gain a more complete picture of an organisation's KM activities.

Practically, I aimed to use an interpretive case-based analysis approach, by conducting semi-structured interviews with various participants within each organisation. The approach followed would focus on discussions with relevant key individuals about how their organisation's KM programs are structured and to indirectly determine whether knowledge and security are treated as wholly separate functions in practice. This was based on my initial assumption that KM and security are largely treated as separate entities in practice. It was also done to help confirm or deny the results outlined in Chapter 5 concerning the relationship between academia and practice. Finally, this approach would help to provide further inputs for the development of the conceptual model.

While this method seemed like a plausible approach to finding participants, practically, it did not yield much in the way of results. Most of the companies that I contacted were not able to put me in touch with the appropriate people, and my contacts were not able to assist in finding many appropriate individuals at the desired organisations. In some cases, where they were able to find appropriate individuals, these individuals were not willing to participate. In total, including the other methods I discuss to follow, I contacted approximately 170 individuals. Given the limited time and resources available, I was concerned that I would not be able to find an adequate number of participants. Following consultations with two senior business professionals^{878 879} and my supervisors, it was decided to tackle the problem by taking an expert centred approach in three ways: 1) By expanding my search approach to include using LinkedIn's paid search and contact services. 2) To expand my reach to include experts from more than two of the identified 15 organisations. 3) To expand my reach to recommended experts, through the snowball technique, residing outside of the 15 identified organisations.

⁸⁷⁶ Heckathorn, 2002. *Respondent-Driven Sampling II: Deriving Valid Population Estimates from Chain-Referral Samples of Hidden Populations* p 11-34.

⁸⁷⁷ Dudovskiy, J. 2016. *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance*.

⁸⁷⁸ Singh, 2020. *Personal Interview*.

⁸⁷⁹ Sudbury, 2020. *Personal Interview*.

With regards to point 1, by using LinkedIn's paid search and contact services, I was able to target key individuals in the organisations of interest, by using search terms such as "knowledge management", filtered by company and region. Through this process, I compiled a list of preliminary individuals for further analysis. From the list, I then opened and scanned through their work experience for relevance to KM activities and roles, any articles, or publications they had posted relating to the topic, as well as their listed skills and endorsements. If identified as appropriate, I proceeded to shortlist them, culminating in sending them a brief introduction via LinkedIn's paid InMail service.

This process seemed to offer a higher response rate than my previous attempts for a few reasons. Firstly, where possible I used individuals' articles and publications as a talking point to get the conversation going, which also proved very insightful. Secondly, for some individuals, we had worked in the same companies at different times and had this as a shared connection. Thirdly, for some individuals, we had shared second or third level contacts who they knew and were, therefore, more open to seeing if they could assist. Fourthly, in some instances individuals had academic work experience and were aware of the challenges faced by student researchers in finding participants. Fifthly, some individuals were interested in doing or had done their doctorates and were keen to find out more about the research process.

With regards to point 2, by expanding my reach to include experts from more than two of the identified 15 organisations, I was able to extend my reach. While I would have liked to find the relevant numbers of participants within the same company, it proved to be difficult due to the structure of their organisations. In most of the organisations contacted, their KM functions were segmented into different business units that were somewhat insular from one another. Thus, most of them did not have enough team members in their immediate networks, within the same organisation, that met my criteria and who could participate in interviews. In some instances where there were adequate numbers, certain members who they approached to assist did not follow through with the interview process. This was largely because those members had limited time available due to heavy workloads.

With regards to point 3, by expanding my analysis to recommended experts residing outside of the 15 identified organisations, I was able to get further participants and get some unique insights. Taking this approach tied up with the constraints of having too few willing participants within the selected organisations and served as a mechanism to overcome this. The individuals who I spoke to in this regard were in most cases referenced to me by the participants in the top

KM companies. These were people they thought were leaders in the field and who they rated as highly competent experts.

I considered that these points were justified modifications to overcome the challenges faced without drastically compromising the integrity of the research. As per the literature, this is also a justifiable approach to take, given that the fundamental objective of this phase of the research was to gain an understanding of KM and security issues from experts in practice. Thus, from a theoretical perspective, I based these modifications on the underlying principle of the purposive sampling technique as applies to qualitative studies. Patton states that it is mostly “used in qualitative research to identify and select information-rich cases”⁸⁸⁰. Further, Etikan *et al.*⁸⁸¹ explain that purposive sampling is a deliberate choice on the part of the researcher to find participants with relevant qualities considered to be important for the research. As Ilker states, the researcher finds participants who “are willing to provide the information by virtue of their knowledge or experience”⁸⁸². Participants are thus identified based on how well-informed they are about the topic of interest⁸⁸³ and on their willingness to participate⁸⁸⁴. While not a perfect solution, as Carson *et al.* discuss⁸⁸⁵, relevance to the research questions rather than representativeness should be the primary criterion when selecting cases. Thus, based on this recommendation, I deemed it an adequate approach to garner appropriate individuals with deep experience in the field, in line with my research objectives.

Some key points relating to the structure and profile of the final participants are summarised as follows:

- Fourteen individuals initially agreed to participate, with nine following through with the final interviews,
- Six of the participants were locally based and three were internationally based,
- Seven of the participants were director level and two were senior management level,
- Six had experience in at least one of the 15 listed organisations and three did not, but still resided in large organisations,

⁸⁸⁰ Patton, 2002. *Two Decades of Developments in Qualitative Inquiry: A Personal, Experiential Perspective* p 261-283.

⁸⁸¹ Ilker, 2016. *Comparison of Convenience Sampling and Purposive Sampling* p 1-4.

⁸⁸² Ilker, 2016. *Comparison of Convenience Sampling and Purposive Sampling* p 1-4.

⁸⁸³ Cresswell & Clark, 2017. *Designing and Conducting Mixed Method Research*.

⁸⁸⁴ Ilker, 2016. *Comparison of Convenience Sampling and Purposive Sampling* p 1-4.

⁸⁸⁵ Carlsson & Turban, 2002. *DSS: Directions for the Next Decade* p 105-110.

- The average industry experience of the participants was 24 years,
- All participants had some knowledge of KM, with three participants primary focus being on broader information security, assurance, and privacy issues and,
- Five of the participants spoke to me in the context of their organisations, while four participants preferred to speak with me in a general capacity as subject matter experts not representing a specific organisation.

Finally, it should be noted that three of the participants, identified as part of the extended process, knew me from previous interactions such as conferences, classes, or work projects. Ponelis states that this can create a chance for some level of reactivity to occur, where participants have “difficulty adjusting to the researcher in the role of interviewer”⁸⁸⁶. Ponelis states further that while it is impossible to determine the impact of this, “reactivity is unavoidable in research where participants are aware of being part of a study”⁸⁸⁷. Ponelis goes on to explain⁸⁸⁸ that given that qualitative interviews are sensitive conversations where a level of trust is required, having some familiarity can act as a greater positive rather than a negative effect. This positive effect is on the quality of the data gathered due to the increased level of trust in the researcher. From a personal perspective, I believe that any such impact of reactivity was somewhat mitigated. I based this on the fact that I did not have a close personal relationship with any of the participants and had only interacted with them very broadly previously.

6.3 Research Method

With the research paradigm and design forming the base of the approach taken, in this next section, I outline the research method and data collection component, as per the research design and objectives for this section. In the sections to follow, the components of the research method are discussed in more detail. This consists of a discussion around data collection, ethics, the data collection process, analysis, interpretation, and the outlining of the case study narratives.

⁸⁸⁶ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 80.

⁸⁸⁷ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 80.

⁸⁸⁸ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 81.

6.3.1 Data Collection

As stated previously, the objective of the data collection phase was to understand how KM works in practice and if there was any relationship to security. To gain this understanding, a semi-structured qualitative interview process was followed, which is often regarded as a reputed and effective method of obtaining data from experienced organisational elites⁸⁸⁹. DiCicco-Bloom and Crabtree⁸⁹⁰ point out that research interviews are among the most familiar strategies for collecting qualitative data, with less structured interview strategies being a conduit for the making of meaning rather than insular information retrieval. In the case of qualitative case studies, Yin⁸⁹¹ describes interviews as an appropriate data collection method, particularly when examining social and behavioural contexts, as in business studies⁸⁹².

As outlined in the research methodology literature, interviews can take several forms primarily focused around a structured, unstructured, or semi-structured approach⁸⁹³, offering different pros and cons as to their use⁸⁹⁴. According to Ponelis⁸⁹⁵, in a structured interview, the interviewer is restricted to a standardised list of questions from which there is no freedom to deviate. This can be thought of as “a survey that is delivered face-to-face”⁸⁹⁶. While this does improve the consistency of the data gathered and can streamline processing⁸⁹⁷, it limits the exploration of additional topics that may arise during the interview⁸⁹⁸. In an unstructured interview, there is no standardised list of questions, making it possible for the interviewer to cover a broad range of topics. While this provides additional freedom, it can make keeping focus on the topic at hand difficult, leading to increased difficulty in conducting cross-case

⁸⁸⁹ Drew, 2014. *Overcoming Barriers: Qualitative Interviews with German Elites* p 77-86.

⁸⁹⁰ DiCicco-Bloom & Crabtree, 2006. *The Qualitative Research Interview* p 314-321.

⁸⁹¹ Yin, 2012. *Case Study Research: Design and Methods* p 106.

⁸⁹² Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 82.

⁸⁹³ Azarpazhooh et al., 2008. *Structured or Unstructured Personnel Interviews?* p 33-43.

⁸⁹⁴ Low, 2013. *Researching Health: Qualitative, Quantitative and Mixed Methods* p 87-106.

⁸⁹⁵ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 82.

⁸⁹⁶ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 82.

⁸⁹⁷ Azarpazhooh et al., 2008. *Structured or Unstructured Personnel Interviews?* p 33-43.

⁸⁹⁸ Clifford et al., 2010. *Key Methods in Geography* p 103-115.

comparisons⁸⁹⁹. Ponelis explains⁹⁰⁰ that in a semi-structured interview, elements of each are combined to strike a balance between rigidity and flexibility. Instead of an interview schedule, an interview guide is used which comprises a list of themes or general questions based on the conceptual framework that has a bearing on the research objectives of the interviewer, should the participant not raise these themselves⁹⁰¹. The benefit of this approach is that it allows the interviewer the option to focus on certain themes in greater depth while being able to address any new areas as they emerge during the interview⁹⁰².

I structured my interview guide around six broad sections, focused on different aspects of my research objectives concerning KM and security. The first section provided context by establishing the participant's broad view of organisational knowledge, the objectives of KM, the role of elements such as structure, culture, the physical environment, and IT infrastructure. The next four sections included general questions relating to the four core KM processes of knowledge discovery, capture, sharing, and application⁹⁰³. These sections were used as a general guide, or where necessary, to provide more information on a particular sub-facet. Not all questions in these sections were asked, as not all were relevant to the different participants' approaches to KM. The final section dealt with questions related to KM and security, to examine any relationships, and to establish any links back to academia. Questions asked in this section were related to the protection of intellectual capital, the retention of people, the role of information security and whether security was a contributing success factor in KM. The interview guide with the themes and questions is attached as Appendix A.

Practically, the interview questions were not followed linearly and were asked when more information was needed, or where a participant did not cover a certain area where more clarification was warranted. Yin⁹⁰⁴ suggests that semi-structured interviews should be more of a guided conversation than a structured enquiry. While in some cases I probed deeper into certain issues, I did so to stay within the scope of the research objectives. Carson *et al.*⁹⁰⁵ explain

⁸⁹⁹ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 83.

⁹⁰⁰ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 83.

⁹⁰¹ Welman *et al.*, 2005. *Research Methodology*.

⁹⁰² Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 83.

⁹⁰³ Becerra-Fernandes & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 66.

⁹⁰⁴ Yin, 2012. *Case Study Research: Design and Methods* p 106.

⁹⁰⁵ Carlsson & Turban, 2002. *DSS: Directions for the Next Decade* p 105-101.

that while providing space to explore new issues that emerge, this has the effect of allowing the researcher to recognise when something important has been said as well as to keep the interviews focused to facilitate cross-case analysis. Additionally, Rowley⁹⁰⁶, as cited in Ponelis⁹⁰⁷, outlines that much of the success of the data collection process relies on the abilities of the interviewer. By this, Ponelis means asking the right questions, asking probing questions, listening carefully, not judging participants' answers or asking questions the participant does not understand⁹⁰⁸.

To mitigate some of these practical concerns, and to ensure I was able to conduct the interviews more appropriately, I set up three trial interviews with friends who had experience working in large organisations. I used these as an opportunity to work out any problems with the set-up used, to get used to asking the appropriate questions and listening, and to gain feedback from them about what areas could be improved upon before conducting the real interviews. Their feedback was useful in the refinement of the interview process and helped me to develop a more streamlined approach. I supported this further by watching training material on how to conduct effective interviews^{909 910} and worked through my university's online training material relating to the interview process and ethical considerations⁹¹¹.

6.3.2 Ethics

The initial assumption made during the proposal phase of the project was that organisations or members of those organisations would not be willing to divulge information relating to their KM or security activity, as this could be a competitive advantage. Upon discussing this further with business professionals for advice, during this phase of the research, it was apparent that assurances of privacy and confidentiality would be an important factor to potential participants. Further, in addition to privacy and confidentiality, when conducting the ethics evaluation, four other key risk areas were also identified and considered. These were psychological risks, social and economic risks, legal risks, and participant inconvenience. While all these risks were

⁹⁰⁶ Rowley, 2002. *Using Case Studies in Research* p 16-27.

⁹⁰⁷ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 85.

⁹⁰⁸ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 85.

⁹⁰⁹ Quirkos, 2019. *Using Semi-structured Interviews in Qualitative Research*.

⁹¹⁰ Chrzanowska, 2014. *Demonstration Qualitative Interview - How it Should be Done* [Online].

⁹¹¹ Stellenbosch University, 2020. *Postgraduate Skills Development Online Training and Courses* [Online].

considered low for participants, I did institute measures to mitigate risk and maintain trust where possible.

Firstly, concerning the mitigation of data privacy and confidentiality risks, I aimed to ensure that the information presented in any publications is anonymised. I made provisions to secure any interview recordings and notes and did not share them with any third parties. I only kept the original data for as long as was needed to finalise the research. Additionally, I gave participants the option to have their data deleted, should they have chosen to withdraw from the study before the publication of any results. Secondly, concerning psychological risks, I informed participants that they may request that the interview be stopped at any stage and that they had the right to refuse to answer any questions with which they were not comfortable. Additionally, if they were not comfortable with the interview medium or the location, they were free to suggest better-suited alternatives. I informed them that none of their actions would count against them negatively. Thirdly, concerning social and economic risks, I informed participants that they were under no obligation to do anything that they felt would undermine their integrity, privacy, or confidentiality. They were also informed that they could request to inspect any transcripts made before publication. Fourthly, concerning legal risks, no interviews were conducted without their express permission, and none were to be included in the results if additional written permission was not obtained. I gave participants the option to ask questions about the documentation and make any amendments to their satisfaction. Fifthly, concerning inconvenience risks, I gave participants the option to conduct the interviews at a time and place that they deemed convenient for them, and I tried to keep the interviews within the agreed-upon meeting window.

Following Stellenbosch University's research ethics requirements, to collect data from human subjects, I submitted an ethics application through the *Research Ethics Committee for Social, Behavioural and Education Research*. This was approved unopposed on 26 June 2020, with project reference number 16552. The application included the following: an overview of my project, participant selection, the process of obtaining informed consent, the risks and benefits of participation, a data management plan, a data collection plan, an evaluation of my documentation and question guide, and the overall project risk classification.

6.3.3 Data Collection Process

The initial requests to participate in my research were sent out to potential participants on 23 May 2020, on the provision that my ethics application was approved by the university.

However, due to the implications of the coronavirus disease 2019 (COVID-19) outbreak and the resulting delays from both the university and the participants' side, I was only able to get the first participant to agree to an interview on 3 September 2020, with the final participant being interviewed on 21 October 2020. Due to the health risks posed by the virus, as well as differences in geographic location, all the interviews were conducted via voice or video chat, usually from the participants' homes, using telecommunications software. On average, each interview took 30 to 45 min to complete. All participants permitted me to do an audio recording of the interviews before proceeding with the discussions, which I did by using two voice recorders to mitigate the risk of equipment failure. As I was not reliant on having to take physical notes to record the interview, I attempted to keep it to a minimum. I did so to not distract from the interview discussion and to keep the flow of the interview going. While taking physical notes can be beneficial⁹¹², it can also be somewhat detrimental to the flow of the interview. Muswazi and Nhamo⁹¹³ discuss that in some settings an observer taking notes might distract participants or cause the interviewer to miss important points. Additionally, note-taking may also disrupt the effectiveness of communication between the interviewer and the participant⁹¹⁴. Thus, as the interviews were already done online, I decided to rather focus on using the audio recording equipment so as not to create further barriers to the engagement.

Before conducting the interviews and in addition to the ethics documents, some of the potential participants wanted to know more about who I was and the details of the research project. In such cases, I arranged an introductory call with the potential participant, where I could answer their questions and give them more details about the research project. I found this to be a beneficial step, as doing so allowed me to establish rapport with the participants and increased our engagement during the full interviews. In some cases, there was no introductory call, so I used the first 5 to 10 minutes of our discussion to help establish rapport and explain the purpose of the research. I also used this time to answer any questions relating to the required informed consent and gatekeeper documents and any other ethical considerations.

Upon completion of the interview, I thanked the participants for their time and stopped the recordings. I sent a thank-you note to all participants via email or messaging service and informed them that I would send them copies of the dissertation and relevant findings upon completion of the project. It should be noted that all the participants offered valuable insight

⁹¹² Muswazi & Nhamo, 2013. *Note Taking: A Lesson for Novice Qualitative Researchers* p 15.

⁹¹³ Muswazi & Nhamo, 2013. *Note Taking: A Lesson for Novice Qualitative Researchers* p 15.

⁹¹⁴ Muswazi & Nhamo, 2013. *Note Taking: A Lesson for Novice Qualitative Researchers* p 15.

concerning KM and security issues. They also went out of their way to be helpful and assist me with identifying further participants. The time they devoted to this was very much appreciated given how demanding their work schedules were.

6.3.4 Analysis and Interpretation

In terms of analysing and interpreting the data, I chose to use Cope's 4 levels of analysis⁹¹⁵, applied where relevant to my research, with the additional 'Level 0' being the interview phase as outlined by Ponelis⁹¹⁶. These levels of analysis were handled iteratively and consisted of "transcribing and capturing notes; writing up case study narratives and within-case analysis; determining findings through cross-case analysis; and interpreting and enfolding the findings"⁹¹⁷.

These levels are summarised briefly in the paragraphs to follow, relating to my approach, as taken from the overview provided by Ponelis⁹¹⁸:

- **Level 0: Interviews** – The process of inductively analysing data commences as soon as the researcher starts collecting the data during the interview phase. During the interview phase, the dual roles of interviewer and researcher co-exist with the researcher engaged in analysing and interpreting the perspectives of the participants, while simultaneously being the interviewer. It is for this reason, that the primary researcher should conduct all the interviews where possible. It was thus to my benefit that I was able to conduct the interviews myself.
- **Level 1: Transcription and capturing notes** – With the data collection completed, Level 1 comprises analysing the transcripts and notes which is a crucial step of data analysis. The transcription of interviews falls somewhere on the continuum between naturalism, capturing all utterances, and denaturalism, removing idiosyncratic elements of speech. For my transcriptions, I chose to follow a denaturalistic approach as I was more concerned with the classification of the core thematic outputs from the interviews. I thus took the audio recordings made during the interviews and transcribed them

⁹¹⁵ Cope, 2005. *Researching Entrepreneurship Through Phenomenological Inquiry, Philosophical and Methodological Issues* p 163-189.

⁹¹⁶ Ponelis, 2015. *Using Interpretive Qualitative Case Studies for Exploratory Research in Doctoral Studies: A Case of Information Systems Research in Small and Medium Enterprises* p 541.

⁹¹⁷ Ponelis, 2015. *Using Interpretive Qualitative Case Studies for Exploratory Research in Doctoral Studies: A Case of Information Systems Research in Small and Medium Enterprises* p 541.

⁹¹⁸ Ponelis, 2011. *An Exploratory Study of Business Intelligence in Knowledge-Based Growth Small, Medium and Micro Enterprises in South Africa* p 89-91.

according to their main thematic points. To analyse the transcripts, I read through them and grouped their content on a case-by-case basis according to these chosen themes. This was useful as it helped to streamline the evaluation and analysis of the interview data.

- **Level 2: Case study narratives** – The transcribed notes are then compiled into a narrative for each case. These are in a form that functions as a readable, descriptive picture of the information necessary to understand the case as it pertains to the inquiry. These can be presented chronologically, thematically, or both. In my research, I chose to structure and present my narratives according to the themes discussed in line with the objectives of the research. As such, they were structured along the lines of examining the role of KM, security and KM, their alignment with academic teaching and additional inputs and considerations from each of the participant's perspectives. I did this to be able to present the interview data logically and to enable an easier analysis of the cases.
- **Level 3: Cross-case analysis** – Cross-case analysis consists of comparisons between the different cases to identify coherent and important themes and patterns in the data. Through this process, the identification of general and unique themes can be gleaned by analysing the cases for topics that recur and those that are unique. The outcome of this level of analysis is the findings derived, based on the data collected. In my case, as I had structured the case narratives according to their themes, the analysis was simplified, and the results of the cross-case analysis were presented and discussed as part of the general summary. This was done relating to their alignment with the research objectives.
- **Level 4: Interpreting and enfolding the findings** – In cases where the findings are clustered together, without the use of any relevant theoretical literature, these findings are discussed in the context of extant literature, or enfolding literature. Thus, the outcome of this level of analysis is the subjective interpretation of the findings as discussed in the context of extant literature. In my case, as I had already discussed the theoretical literature concerning knowledge, KM, knowledge security and practically examined academic teaching, I determined that the results of the cases presented did not need to be associated again with the theory. Additionally, as I was aiming to examine the findings in terms of the stated research objectives, their outputs were used to decide upon the validity of my initial hypothesis.

6.3.5 Case Study Narratives

The cases are presented in the sections to follow and segmented according to two main themes. These are the role of KM in organisations and the relationship between security and KM. Both are framed from the participant's perspective based on the feedback they provided. The case study narratives form the basis of the discussion to follow in terms of determining any alignment with academic teaching as discussed in Section 6.4. Any additional inputs and considerations mentioned by the participants, not within these initial two broad themes have been excluded in this section. These are summarised and discussed separately when dealing with the analysis of the findings in Section 6.4. Cases A-E consist of the input from those participants who have a primary focus on KM roles, while Cases F-H consists of input from those participants who have a primary focus on security roles. For Case B, as the participants were from the same organisation, their findings were condensed into a single case.

6.3.5.1 Case A - Participant 1

Role of KM – In the participant's organisation, knowledge is managed using a KMS. The purpose of this is to support the employees by allowing them to find relevant content or experts when working on consulting projects. They need to be able to land projects by writing effective proposals and to collaborate efficiently with team members when executing client proposals. They view IP as critically important to their success. As such, they focus on codification processes, aligned with a defined KM strategy and supporting technologies, to capture and use their knowledge.

Security and KM – Their security activities focus on protecting their KMS, underpinned by information security principles. Their KMS is governed by risk controls that determine how knowledge is handled by employees and who has access to it once it has been codified. This takes the form of technical security mechanisms, role management and accountability based on employee seniority within a project. For the knowledge contained in the system, client confidentiality is seen as key. To ensure confidentiality, any knowledge added to the system goes through a sanitisation process to remove all client identifiers. Employees are also trained on how to ensure client confidentiality is maintained when interacting with other clients or in public contexts.

6.3.5.2 Case B - Participants 2 & 3

Role of KM – The participants’ organisation views knowledge as critical to their operations and takes a systems and culture approach to KM. This is determined by the individual requirements of their respective business units and is embedded as part of their processes. The focus of their KM activities varies accordingly with a focus on content management in some units, the development of proposals for customers and knowledge harvesting for quick problem solving. From a systems perspective, the primary aim is to connect people and content using a framework based on the KM principles of tacit knowledge, explicit knowledge, and meta-data definitions. This framework governs how people deal with knowledge in the organisation. To actualise this, the organisation makes use of COPs and has cultivated a culture that is focused on sharing to drive knowledge collaboration. To ensure this, the organisation has made it a requirement of their employee rewards model. The rewards model is associated with performance management and is based on expected targets for the generation, sharing and consumption of knowledge.

The organisation also has a strong emphasis on the adoption of AI, neural networks, and machine learning as part of its KM approach. They do so in several ways. Firstly, they use these tools to reduce the administration load associated with knowledge sharing, due to the rapid rate at which their data grows. Secondly, they use these tools to assist with knowledge discovery in their information and knowledge systems as it can illuminate new patterns which can help these systems to better “understand” the knowledge contained therein. Thirdly, they integrate these elements into their COPs so critical IP is not left behind when consulting with customers or in their general business practices. Fourthly, they use these tools to spot trends in their knowledge, taken from multiple inputs, to assist with things like budgeting.

Security and KM – The organisation views the security of their knowledge as important to organisational performance. Their security activities are focused on the protection of their IP and KM is governed across all business units. The organisation’s IP management strategy is structured around business-critical, community and individual level IP. They focus on what knowledge is critical to the business as they realise that they cannot capture everything. The business-critical IP is embedded in the organisation’s business processes and is highly structured and maintained through strong quality assurance processes. The community and individual level IP are less formally governed and are rather driven by the needs of the relevant COPs.

From a practical security perspective, the organisation focuses on stringent KMS security controls, underpinned by information governance, information security, risk aversion, legal and compliance requirements. These elements are integrated into their policies and processes. Knowledge in their systems is classified according to a governance framework in terms of high, medium, and low business impact. The organisation uses this governance framework to automatically determine the level of access to knowledge according to the employee's role and business function. These governance processes also help to automatically determine the classification of documents.

From an AI perspective, the organisation makes use of automatic security tools to monitor its systems by looking for unusual patterns and spikes in behaviour. If found, the system will notify their security team about the problem. In certain situations, where the organisation holds highly confidential meetings, they will use machine learning security tools to monitor people's activities to ensure that they do not share or capture anything they are not supposed to.

Additionally, all employees undergo security training several times a year which focuses on how to identify and manage things like social engineering, phishing, email scams, maintaining confidentiality in social situations and identifying insider threats. This training forms part of their conditions of employment. Finally, in some instances, the organisation will force certain key individuals to go on paid leave for six months before starting a new job at a rival organisation. They do this to ensure that the critical value of the knowledge the employee has will have diminished, or to allow their organisation time to establish market dominance should the value of the employee's knowledge not be diminishable.

Most of their work was focused on short-term projects and project teams, with employees typically remaining in a role for 18-24 months. They indicated that due to the nature of their business, workforce skills change fast and what they do is designed for obsolescence. The participants indicated that they felt that the approach they take is proactive and works well. In their view, it is effective in getting critical IP from people by capturing this knowledge through their IP process models. This is then formalised into those things that will have long term business value and the highest impact on the organisation. Finally, they indicated that if there are any issues with the induction of new employees into a role, they are still able to access the organisation's COPs to consult with people who have those original skill sets.

6.3.5.3 Case C - Participant 4

Role of KM – From the participant's view, KM should be positioned as a centralised function, coupled with an organisation's governance processes for a couple of key reasons. Firstly, it will ideally result in a blanket set of rules that govern policies and standards documentation. From the participant's experience, not having this in place can lead to fragmentation and ultimately the capturing of low-quality knowledge in an organisation's systems. Secondly, it can make finding experts more difficult, thus resulting in the re-inventing of solutions that already exist. The participant indicated that KM is a function of business strategy and should only be implemented when it makes sense to do so. They noted that the objective of KM is to pull together a lot of smaller practices, but that this will be highly contextual as not every process will be applicable in all cases. They indicated that KM also helps to define the culture of the organisation in terms of how people work and engage with content.

Practically, this is actualised by having tools in place that function well and are easy to use. For example, this can mean having relevant COPs which are combined with well-defined policy and processes to ensure the CIA of the knowledge being captured in their KMS. For the participant, KM needs to be supported by a good organisational structure and must be driven by people on the business strategy side too. From the participant's experience, the requirement to share knowledge should not be motivated by financial rewards. Rather, there needs to be a culture of sharing created that is motivated by helpfulness and a desire to want to assist one another.

Security and KM – From the participant's experience, the measures that they observed were highly governed by IT and information security policies, with less emphasis being placed on the softer non-technical elements. There was also a heavy emphasis placed on compliance and some risk management, but only in so far as it related to meeting compliance requirements for the industry. The participant noted that the products they develop for customers are highly secure, but the mechanisms and IP used to develop that was not something to which the organisation was overly attached. The important things were customer information and some work information related to interactions with customers. Anything created inside the organisation, from a knowledge and innovation perspective, was not seen as that valuable.

The participant explained that the capturing and retention of knowledge, from experienced people, was focused on intensively in certain parts of the organisation. The objective of this was to be able to reuse their knowledge for business projects. However, in other parts of the

organisation, there was not such a focus, resulting in a lot of re-inventing of things. The participant mentioned that this is very industry specific and will depend on the kinds of projects and employee turnover the organisation has. From their experience, based on the organisations they have worked for, it would not be hard to induct a new person. They stated that this was because the projects they worked on would not require the intensive transfer of intellectual knowledge. They indicated that this could be done through training or by providing the new employee with what had already been documented.

6.3.5.4 Case D - Participant 5

Approach to KM – In the participant's organisation, knowledge is managed through a combination of cultural interventions and a strong focus on document and KMS tools. They view knowledge as something that exists beyond an employee's head and is part of the broader organisational community. The organisation has long-established COPs which allow employees to find best practices and have technical questions answered. The organisation works on large long-term projects, that can extend for decades, and is therefore heavily focused on managing IP as part of their KM strategy. On a project basis, their KM focus is on capturing high impact lessons from previous projects. The organisation has hundreds of approved subject matter experts who are high-level experts in their field and have a lot of access to knowledge. As part of this, they aim to foster a culture of sharing, where captured knowledge is vetted by these high-level experts, as the integrity of the knowledge captured in their systems is extremely critical to safely executing their projects for clients.

The organisation also focuses on a process of continuous learning since the projects they deal with are so extensive. The participant indicated that doing so at the end of a project does not work as many project members will be gone or will not remember what they did given the long timeframes. From a KM perspective, they try to prompt employees as they learn things or submit things of significance so new project teams and employees can learn from them. As their KM strategy is culturally driven, no financial incentive is given to employees to participate in the program. Rather they focus on getting people from different areas of the organisation to talk to and help one another.

Security and KM – From a technical perspective, the participant indicated that the organisation has a heavy focus on security as the industry in which they operate is very secretive. Their chosen security approach is one governed by information security, as most of the attacks they face are aimed at compromising their information and knowledge systems. The

organisation thus focuses on having extremely strict IT systems security controls in place. These controls are centred around protecting the client IP that resides in their systems.

When considering confidentiality, the organisation examines who will be allowed access to any of the knowledge that has been generated. For example, for each phase of a project, they determine who needs to know what knowledge. Once determined, this is segmented according to an employee's level within the organisation. They also aim to share just the right amount of knowledge with the right people both forward and backward in the project process to limit and control the knowledge. Access control to the project information is shared only with those who are working on the team. Additionally, one primary team is responsible for the project roadmap and management of the project. They then split the relevant sections of the project into chunks and assign different project teams for each of those chunks. The participant indicated that there is also a focus on risk, but that this is framed in terms of the legal ramifications of making mistakes in their projects or security.

From a cultural perspective, concerning the security of their COPs, they take a common-sense approach to trust. By this, they aim to trust that people will learn from the culture of the company what is expected of them and not do or share things they should not when collaborating. In those rare instances where people have shared knowledge they are not supposed to, they are quickly corrected. The organisation does this in a kind, non-critical way through feedback from other employees of the organisation. Thus, the participant indicated that new employees would learn this common-sense approach, as it is the culture of the company. The participant also noted that most of what is discussed in their COPs is related to the technical challenges with the products they provide and is rarely client specific. The participant indicated that new employees would soon see the general trend of what is expected behaviour and that they would realise what is appropriate.

Due to the nature of the projects that the organisation works on, the participant indicated that they do take measures to counter the loss of experts. To counter the loss of experts, they have a program in place that identifies the next experts, with 3 to 4 per category, who are then integrated through an induction process. The organisation also aims to build a culture that allows people to thrive and learn because, as the participant indicated, the exit interview stage is too late. They consider this a better approach as buying in experts can be expensive. They also have job level tracks for people to gain and grow in experience and a learning platform with hundreds of online courses.

6.3.5.5 Case E - Participant 6

Approach to KM – In the participant’s view, KM is required to democratise knowledge. Thus, the objective of KM programs is to take on the overarching responsibility for the management of tacit and explicit knowledge in an organisation. This is achieved through a variety of systems, tools and management techniques which include implications for information management and records management too. This is because, in the participant’s view, KM functions as an umbrella term that encompasses these and other disciplines too. The KM team is also responsible for defining several elements in this regard: the collaboration platforms used, ensuring that activities are aligned with regulatory requirements, how knowledge is to be used, how COPs should manage their content, how the intranet is used, and where high-quality documents must go.

Security and KM – From the participant’s view, knowledge security is important. It should lead governance in terms of knowledge protection, which in turn should lead projects to do with the promotion of access to information. The participant discussed that from their experience, it is especially important to look at how securing knowledge will impact KM programs. They outlined that this is because knowledge security is different to information security, as it not only focuses on the explicit but also on the people of an organisation.

From a technical knowledge security perspective, security is more tangible, as it can be focused on securing an organisation’s information systems. As such this would involve the application of information security controls, records management, and classification principles. They also control access rights based on seniority, job role, project role and project scope in the workflow process. Access to knowledge, in this regard, is defined at a project level by the information management, KM team or various experts including records management. This includes what knowledge should be made public, internal, confidential, or top secret etc. and what those things mean for employees when dealing with knowledge. Knowledge captured in the system should also be managed by a specific team and go through a refinement and approval process before being published.

From a non-technical knowledge security perspective, the participant indicated that organisations also need to train their employees about what should and should not be shared, and particularly how to counter things like social engineering and so forth. Otherwise, sensitive organisational knowledge could be disclosed unintentionally. The participant mentioned that an organisation should also focus on not keeping any knowledge for longer than is necessary.

Additionally, the participant highlighted the importance of having a knowledge transfer program in place to identify the critical knowledge that people are working on. In this regard, they outlined that there is a need to understand the key tasks and knowledge to which the organisation relies. To do this, they examine what sources experts are using to keep up to date, who they interact with and who in the organisation aspires to be like them. They also do so by analysing KMS activity and identifying what people are looking for, what they are sharing and who they are sharing it with. Through these processes, they can identify the future generations of experts, and induct them into the program, partnering them with relevant mentors. Doing so allows knowledge to be transferred tacitly beyond the explicit and to ensure continuity should an expert leave the organisation.

From a social perspective, the participant explained that organisations need to have strong processes in place to force people to share and convert personal knowledge into organisational knowledge. This is done to mitigate knowledge security risk through harvesting and transfer processes. Risks can include employees only superficially sharing some of their knowledge, keeping valuable knowledge to themselves, or developing profound solutions and then leaving the organisation. To counter this requires an in-depth understanding of what employees are working on. For example, the KM team might aim to identify employees who work on their own and develop valuable solutions but do not share their knowledge of how they do this. If their knowledge is not harvested and transferred, they can in essence hold the organisation to ransom. This is because they know the organisation would not be able to let them go without significant loss.

6.3.5.6 Case F - Participant 7

Approach to KM – From the participant's experience, what is considered knowledge in an organisation will vary depending on the context in which the organisation operates. Additionally, the participant noted that this can also vary depending on the spectrum on which it is observed. This is in terms of the transition from data to information to knowledge. Thus, what might be considered knowledge in one organisation can differ from what will be considered knowledge in another organisation. With this view in mind, the participant indicated that for them KM should be based around the organisation's business initiatives as required and can be examined from an integrity and availability perspective, as this links up with the core principles of KM.

Practically, the participant observed that there were attempts made in the organisations they worked for, to capture working papers, standard operating procedures (SOPs), train other members of staff, capture experiences and the engineering of COPs to codify performance management procedures. Participation in the KM program was motivated by soft rewards rather than financial rewards. The participant noted that this sometimes created a problem, as it was up to individual employees to initiate knowledge sharing and take things forward with their teams. Thus, potentially creating a lack of consistency in implementation if the individual was not willing to champion the initiative as much.

Security and KM – The participant noted that in terms of security and KM, there is a lot of focus on protecting IP and that litigation readiness is a big part of that, either to protect former employees from suing the organisation or to sue employees for disclosures. The participant discussed that organisations could focus on the protection of IP from multiple perspectives and recommended taking an integrated approach, considering things like litigation readiness, financial exploitation, diversified income streams, current management, political context, and staff happiness, etc. They indicated that the organisation's leadership would help to determine what the balance is between these different aspects. Each organisation would have a different view and do things according to their approach.

The participant frames security issues from a risk management point of view and outlined that security can be both an enabler and a barrier to KM. For example, as an enabler, security can drive data quality and ensure knowledge is up to date. It can also enable staff to actualise things like better privacy controls and provide the motivation to maintain these controls. As a barrier, when dealing with legislation and IP, particularly concerning cross-border negotiations, the participant noted that in some cases delays to contracts and work outcomes were caused. This was because the legal firms they were dealing with would apply the same stringent default clauses across the board. This meant that often there were clauses in the contracts that did not apply to what was being requested and would hinder progress.

In some of the participant's recent roles, they have been focused on managing privacy issues. Thus, they take this view when thinking about information and knowledge security governance. For the participant, what makes the implementation of security and privacy difficult is that it needs to be understood in the context in which it is used. The value that knowledge holds should correlate between the value of that knowledge for the organisation as well as for malicious users. How long this knowledge will be of value to either party should also be considered, as well as that value in context. The participant indicated that things with the highest classification

level should be considered as the pinnacle of knowledge. Thus, if it is easy to launch an attack against something currently valuable, the more harmful the attack and the bigger the impact.

The participant outlined that knowledge should be classified according to a classification framework, but that there can be many complexities associated with doing so. Using the example of personal information, in certain contexts the participant noted that that same personal information may be considered both public and private. Apart from the complexities of classification, the participant outlined that anything that an organisation decides to implement in this regard should be implementable. Additionally, compliance checks should be put in place to ensure correct classification in terms of how employees understand what is considered confidential and what is not. The participant noted though that the focus should not just be on compliance but rather where things like compliance are a by-product of doing other security activities well. Frameworks can be used to identify security gaps in an organisation's KM activities, which should be in line with an organisation's policies and internal requirements. An organisation can also use approaches from one framework which will then by default cover another. From that point, the organisation would then aim to fill in the gaps where needed.

Finally, the participant discussed that losing key employees is a risk and is often driven from two perspectives. Firstly, where employees have exportable skills combined with increasing push-pull factors external to the organisation. In these cases, the participant mentioned that attempts can be made to outright retain these employees through increased compensation. Secondly, where employees are highly skilled but are not able to integrate with the culture of the organisation. In these cases, the participant mentioned that attempts can be made to integrate employees with the cultural fit and expectations of the organisation. If this is not possible, it is often better to let these kinds of employees go, as it can create too much internal conflict.

6.3.5.7 Case G - Participant 8

Approach to KM – For the interview, the participant purposively chose to frame the discussion on the process of securing knowledge and how that works from their experience. The participant did have a grasp of core KM principles but felt it would be best to focus the discussion in this way. This was likely due to the participant having a strong security background in addition to broader organisational experience.

Security and KM – The participant began by highlighting the importance of identifying what knowledge within the organisation needs to be protected. For the participant, this would include any knowledge that is business-critical, and which makes the organisation unique in the competitive landscape. From a KMS security perspective, they handle this by having a classification system, as defined by the knowledge manager, that would be enforced with relevant controls. Doing so allows for the identification of sensitive knowledge, its categorisation, and what protection mechanisms would be required. From the participant's experience, this is when information security would come into play and would suggest the required controls for the types of classifications that have been defined. The participant discussed that from a security standpoint, this process should be a collective effort with ultimate responsibility remaining with the organisation's head of security.

In terms of the security mechanisms to apply, the participant explained that this should also be governed by the risk profile of each organisation. The risks need to be identified, understood, and prioritised to know which of the risks are most critical and need to be eliminated first. These decisions would be based on the likelihood of something going wrong and what the impact of that would be for the organisation. The participant emphasised the importance of always evaluating your organisation's risks first and then looking at what standards to apply to mitigate those risks. The participant also highlighted that following a particular compliance framework alone can lead to a false sense of security. This is because it can potentially create some security gaps, which may increase the risk to the organisation.

The participant outlined that there are no defined controls to protect someone's tacit knowledge. Rather they suggested focusing on the security principles of least access, NDAs, restraint of trade, policies and processes governing sharing practices to protect the organisation's IP. The participant indicated that the balance of this protection will differ from one organisation to the next. Further, the participant mentioned that if people share knowledge, it will get transferred into their heads. Thus, the only real way to deal with this is through contract management and to hold people accountable to those contracts. Such contracts should be signed before a new employee starts their job and should be part of the organisation's onboarding process. An additional control is that an organisation should aim to keep its employees happy. They should be paid appropriately for their skills as it may increase loyalty and keep key employees with the organisation longer, thus limiting the effect of knowledge loss.

In terms of an experienced employee leaving, for the participant, this is not such a risk. From their perspective, the likelihood of this happening is high, but generally the impact is low. The participant mentioned that employees who remain may struggle for a while, but they would be able to figure it out, provided there is some support in place. Ideally, according to the participant, it is important to capture SOPs so for those who remain there is something to follow. Additionally, they mentioned that there should also be other employees shadowing experts to learn how things are done. The idea is that if the expert leaves, the shadow employee can take over their activities. For the participant, this is a good approach to knowledge transfer, to keep the engine running when someone leaves with specific knowledge. However, the participant did mention that it would still be important to ensure that an employee does not leave with the organisation's IP, or where they have not transferred their knowledge to those who remain.

Finally, for the participant, using the CIA principle can be a good way to assist with achieving a balance between sharing and restriction. The participant noted, however, that each organisation will have a different CIA weighting and amount of access depending on their needs. They also noted that concerning the confidentiality aspect, it needs to be defined. For integrity and availability, these can then be managed using technology tools.

6.5.5.8 Case H - Participant 9

Approach to KM – The participant views knowledge as the collective wisdom of the application of information, or information put to use. From the participant's experience, KM is largely systems focused, acting as a conduit for knowledge sharing and learning to take place. As the participant has a security background, they take a predominantly security-focused approach when considering knowledge and chose to frame the discussion in this way.

Security and KM – Concerning knowledge security, within their current security role, the focus is on securing the organisation's IP in its business systems, in the form of explicit knowledge at rest in systems. The value of the organisation's IP is determined by the business leaders, and once this has been distilled into a product or service, relevant legal protections are then applied. The participant thus views the security of knowledge as an important factor that contributes to organisational performance and success. Broadly speaking, the participant indicated that a value-driven approach is taken to the protection of knowledge in this regard. For the participant, this is focused on maintaining the balance between sharing knowledge and protecting it from a value life cycle perspective. For example, data has value, analysis of that

data adds more value, and as an organisation engineer and applies their collective knowledge into a product, it is hugely valuable. However, the participant explained that once a product is released/patented it is less valuable, as it is hard to protect something out in the public and the organisation has less control over who could reverse engineer it.

Concerning the relationship between security and KM, from a technical perspective, this would have a KMS focus, driven by information security controls. The participant indicated that there should also be a focus on operations security, where employees are trained not to divulge sensitive knowledge. When it comes to protecting an organisation's knowledge assets, the participant explained that while legal protections do help in some circumstances, regarding IP, it is important to remember that malicious entities do not care about legal protections.

Further, the participant recommended that organisations need to be aware that often malicious entities will aim to compromise a human asset in the organisation. For example, a target might be a member of an engineering team that is involved with the distillation of information to create knowledge and a product. The compromised target would then be able to inform the malicious actor on which systems and technologies to focus. From the participant's perspective, the value apex of that knowledge would be right before a product is released, when at its highest, so they could gain a competitive shortcut very rapidly. Once the malicious entity has gained persistence, they would be able to look for themselves and indicate, depending on their objectives, what could either be used to escalate their processes or create a competing product. In other words, what would offer the highest ROI for the attack? The participant indicated that from their experience this is typically the way it is done and is therefore also about compromising the right employees in addition to the right systems.

Lastly, the participant indicated that concentrating important knowledge on a few key people in an organisation is a risk for a couple of reasons. Firstly, they are single points of failure and can carry a lot of critical knowledge around with them tacitly. Secondly, it is hard to manage and keep knowledge in an organisation when it comes to people, as they may come and go. They highlighted that there needs to be a process of knowledge capture in place to ensure that knowledge transfer can take place to subordinates where required. Additionally, they indicated that organisations should be capturing this risk in their business risk assessments if done from the broader business perspective, and that focus should not just be given to malicious entities or natural disasters concerning the organisation's security practices.

6.4 Cross-Case Analysis and Discussion of Findings

In the section to follow, I will discuss some general observations relating to the participants and their feedback. Next, I will outline the feedback from the interview process, relating to the areas found, concerning the security of knowledge in academic programs as presented in Chapter 5. This will be followed by a summary of some additional considerations provided by the participants that may also be of interest to the discussion around modelling knowledge security to be presented in Chapter 7. Finally, I will provide a brief discussion about some of the limitations of the research conducted.

6.4.1 General Observations

Before outlining the findings, I will begin by delving into some of the more general observations relating to the participants and their feedback. Firstly, the level of knowledge about the topic from an industry perspective was greater than expected. While for all the participants it was not a formalised practice, some had considered this issue quite seriously. Secondly, I found there to be a general alignment with the materials being taught in academia but not specifically relating to knowledge security as its own entity or field. Thirdly, the level of insight gained from the participants proved to be valuable in helping to better frame and understand the problem. They provided a great deal of nuance and practical insight, which could not be gained from the academic material alone. In this regard, I think the participants' extensive industry experience was highly valuable, as they had a lot of knowledge and expertise to share which is often not always related to the formalised view of how things operate in practice.

6.4.2 Alignment with Academic Teaching

The feedback provided by the participants during the research interviews about knowledge security issues, as outlined in Chapter 5, has been summarised in Table 6-13. This has been structured in terms of the key areas identified in academic teaching as found in practice, based on the participants' feedback. The areas marked with an "X" in Table 6-13 relate to those elements expressly focused on by the participants during their interviews. It may be that some areas are still covered within their broader organisations or experience, but it is rather a representation of what they chose to focus on during the interviews.

Table 6-13: Alignment with Academic Teaching

Case	Legal Mechanisms	Employee Retention Measures	Archiving Key Knowledge (Explicit)	Transferring Key Knowledge (Tacit)	Information Security Mechanisms	Governance, Risk and Compliance Mechanisms
A			X		X	X
B	X		X		X	X
C			X		X	X
D			X	X	X	X
E			X	X	X	X
F	X	X				X
G	X	X	X	X	X	X
H	X			X	X	X

To begin, the implementation of legal mechanisms to secure proprietary knowledge in organisations, in 50% of the cases, was indicated as a mechanism of knowledge security control. This follows a similar paradigm to that expressed in Chapter 5, where the use of patents, NDAs, contracts, and other similar legal documents was mentioned for this purpose. From the interview process, the focus on these legal control mechanisms appears to be more common with those participants who have a security background. Of the four cases where the legal requirement was mentioned, only one came from a participant who had a focus primarily on KM. This is likely an indication of the difference in focus between a KM view and a security view, where there would be more emphasis on having to meet legal and compliance requirements.

Next, in terms of the retention of key employees through HR management mechanisms, this was mentioned in 25% of the cases. The ratio in popularity of this approach also seems to be in line with that discussed in Chapter 5, where there was some mention of this aspect, but it was perhaps not a primary area of focus. It was somewhat surprising that this aspect was only mentioned by those who had a security focus, with both the participants who mentioned this, coming from a security background. Based on KMs closer strategic alignment with HR

functions in some organisations⁹¹⁹, I would have expected this to be more of a consideration from a KM perspective, particularly when it comes to retaining key experts.

Regarding the archiving of explicit knowledge in systems, this was mentioned in 75% of the cases and relates to those measures found in academic teaching as listed in Chapter 5. All KM focused participants mentioned this aspect, while only one participant who had a more security-focused perspective mentioned it. The balance of this result being in favour of those with a greater focus on KM, as opposed to security, does make sense as knowledge capture is one of the primary objectives of KM⁹²⁰. In a security context, the focus would thus not be so much on the actual capturing processes but rather protecting the explicit knowledge residing within the organisation's relevant IT systems.

Regarding the transfer of tacit knowledge from experts to future experts, this was mentioned in 50% of the cases and relates to those measures found in academic teaching as listed in Chapter 5. It was again interesting to note that there was more of a weighting given to this from the cases examined where the participants had a security focus. The lower occurrence by those participants operating from a KM perspective can be explained by the variance in need for this based on their organisation's focus. Where there were long-running projects, it appears that this aspect was more of a concern as opposed to those organisations with shorter project time frames. Speculating from the security perspective, this aspect might have had greater weight, as needing to ensure continuity is important. Additionally, if continuity is not ensured, the impact of failing at security is much greater. So, it would thus make sense that this would be more of a consideration.

In terms of approaching the topic of knowledge security from an information security perspective, 87.5% of participants mentioned this in some capacity. This was usually directed towards the use of information security controls to protect KMSs and other KM related technology tools. The one case that did not mention this specifically was a participant who had a security focus but framed from a privacy, compliance, and governance perspective. The role played by information security in this capacity aligned with the focus as found in academia in Chapter 5. Given the increased awareness of information security issues⁹²¹, it would make sense

⁹¹⁹ Gloet, 2006. *Knowledge Management and the Links to HRM: Developing Leadership and Management Capabilities to Support Sustainability* p 402-413.

⁹²⁰ Becerra-Fernandes & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 66.

⁹²¹ Wiley *et al.*, 2020. *More than the Individual: Examining the Relationship Between Culture and Information Security Awareness* p 1-3.

that participants who have a KM or security focus would both view this as an important aspect in today's business context.

Finally, while there was some mention of governance, risk and compliance as found in academic teaching, which was discussed in Chapter 5, in this case, 100% of the participants made some reference to this aspect. While it was not always framed from the perspective of knowledge security directly, it did play a role in the determination of security, risk and compliance relating to the mechanisms needed to govern issues around employee roles, access control, and the identification of knowledge at risk. Given that one of the focal points of KM professionals is on systems and other types of KM technologies, it would also make sense that the mechanisms needed to govern these would be considered important to both KM and security-focused professionals.

6.4.3 Additional Knowledge Security Considerations

During my discussions with the participants, they also highlighted some additional areas to consider that may inform the discussion in Chapter 7 concerning modelling knowledge security. These included several aspects, with four of them having been mentioned by two or more participants. The identified aspects are the need for a balance between effective technology and a culture of sharing; instances of security being too stringent; a lack of focus on encouraging innovation by an organisation; awareness of the value of knowledge for malicious entities; and general issues that fit within the CIA triad paradigm.

Concerning the need for having a balance between effective technology and a culture of sharing, the impact of a lack of balance manifested in several ways. Firstly, participants mentioned that if you have good KM technology in place but not a culture that is supportive of using it, the initiative will fail. Conversely, if there is a culture that is supportive of promoting KM but the KM technology in place is weak, it will also fail as employees will not be able to make effective contributions. Secondly, if there is a culture favourable to sharing and the KM technology in place is not streamlined, employees may attempt to come up with their own solutions. This can be on a business level or where the employees still require social connection and so will use non-sanctioned tools for their social communications. In doing so, this can create additional risks for the organisation as these are not controlled. Even after effective KM technologies have been implemented, if the use of non-sanctioned tools has been going on for some time, it may lead to bad habits being ingrained in how employees do things, leading to a continuation of the risk.

Regarding instances of security being too stringent, several examples were given by participants. The first was where employees in a particular function had locked down their KMS, only making it available to themselves. This in turn created a silo, with others in the organisation not being able to access this knowledge. The participant indicated that this had potential implications for the organisation's data mining activities as this knowledge could not be incorporated. The second example given was where change control practices were universally applied across all systems in an organisation. This manifested in non-essential internal systems being subjected to the same level of change restriction as critical client-facing systems. From a KM perspective, this led to delays where they were not able to quickly adapt these internal systems to their needs, as well as downtime. The third example given, as mentioned previously in the case study narratives, was related to contract management, where the same legal templates were applied across all contract negotiations. In some instances, this was required, but in many others, it was not. The participant indicated that this led to delays through unnecessary legal wrangling and a lot of wasted time having to get the irrelevant sections removed.

For a lack of focus on encouraging innovation by an organisation, several aspects were mentioned. Firstly, where knowledge was used to create a customer product, but the organisation saw no value in capturing or protecting the knowledge related to the development of that product or seeing how it could be applied in other ways. Secondly, where innovative solutions were developed by employees that would have saved the company money, but where these were not capitalised on by the organisation. Thirdly, where there was a general lack of focus on innovation in the culture of the organisation and little encouragement to innovate or explore was given. In all these cases, the participants indicated that they saw this as a potential risk to their organisations in the future. These were from the aspects of the organisation missing key trends and developments in the industry, being overtaken by more innovative competitors and then not being able to catch up, or where innovative people were side-lined eventually leaving the organisation.

In terms of needing to be aware of the value of knowledge for malicious entities, the participants highlighted two aspects to consider. The first was that consideration should be given to where in the value chain knowledge will offer the greatest ROI for an attacker. This appears to be organisation and industry-specific but could be, for example, at the planning phase of a project, or just before a completed product has been developed. The second was that

consideration should also be given to how seemingly insignificant knowledge might be combined by an attacker with other pieces of knowledge to become more valuable.

Finally, participants also mentioned several other issues individually, which when combined can be explained from a CIA triad perspective. From a confidentiality view, these include issues relating to oversharing knowledge without consideration of the implications for privacy or security. For example, as outlined by some participants, in social settings outside of work, or where trying to help a customer, another customer's competitive knowledge is inadvertently shared. Further, where an employee may have made a knowledge sharing contribution, but what was shared was compromised reflecting badly on the employee. An additional example also mentioned was where an executive might share sensitive knowledge with someone who should not have the rights to access that knowledge, but due to the delegation of work, or where asking a subordinate for assistance, this knowledge becomes exposed, which can lead to knowledge leaks.

Next, from an integrity view, participants also mentioned how having a low level of integrity of the knowledge in a system can contribute to mistrust by employees and a lack of use. Additionally, where the knowledge in the system, while initially containing value for employees, has been overly sanitised for privacy reasons, leaving what is contained in there of no use to employees. A further example was given by a participant related to the integrity of tacit knowledge. This was from the perspective of the manipulation of knowledge conveyed, the use of deception, or disinformation to meet personal political objectives. This can lead to bad decision making, fraud, corruption and the organisation being held to ransom by critical employees. These employees may have developed profound solutions for the business but have not shared what they know. Thus, knowing they are the only ones who can assist with such solutions, they leverage this to their advantage, as mentioned previously in the case study narratives.

Finally, from an availability perspective, this can extend to situations where employees are not able to gain access to relevant KM technologies, not for a lack of wanting to adopt these but due to external factors like slow internet access. One participant mentioned that due to slow internet access, in certain regions, it was impossible for employees to effectively use the knowledge resources available to them. Another participant mentioned that in some cases there were issues too with the availability of employees to participate in their KM programs. This occurred where employees were so overworked that they had no time to devote to their personal growth and development or to share or consume knowledge through learning activities.

6.4.4 Limitations of the Study

While I did do as much as possible to mitigate the effects of any research limitations, it is important to note that there are still some potential limitations of which to be aware. These include aspects like the potential risk of bias through the interview process or having to modify the range of the participants chosen. I have already addressed these two issues previously in the chapter, and as such I will not outline them again here. However, there are some further aspects relating to the research limitations, which I thought should also be considered.

Firstly, when processing the interview results, to protect the participants' privacy, certain aspects of the discussions had to be rephrased, as presented in this chapter, to ensure anonymity. The implication of this is that this rephrasing may have been influenced by my frame of reference to some degree. Therefore, this could lead to some changes in the original intent of what was expressed by the participants. I did attempt to mitigate this as far as possible by remaining conscious of it and trying to ensure that what I listed reflected the core elements discussed during the interviews. However, as mentioned previously in the chapter, bias cannot be eliminated⁹²² and there is always a possibility that in some instances this may have crept into the results.

Secondly, concerning the open nature of the interviews, there is the potential that discussions leading in a certain direction may also have created a confirmation bias feedback loop. For example, where the interviewer is driving the conversation according to their preconceived notions or where the participant is providing information to the interviewer in a more favourable light, according to what they think the interviewer will want to hear⁹²³. I again tried to limit this by not discarding or re-enforcing any one point, but it is a possibility that I was not always able to remain completely objective in these discussions, even when consciously trying to do so.

6.5 Conclusion

Chapter 6 formed the second and final part of the empirical analysis and aimed at establishing if what is done in practice reflects those elements found in academic teaching and what the relationship between KM and security is in practice. This was in line with the research

⁹²² Salazar, 1990. *Interviewer Bias: How it Affects Survey Research* p 567-572.

⁹²³ Salazar, 1990. *Interviewer Bias: How it Affects Survey Research* p 567-572.

questions as mentioned in Figure 1-2⁹²⁴ ⁹²⁵. To achieve this aim, a qualitative, interpretive research approach was used. This consisted of a series of interviews with leading experts in the field to get further insight into KM and security issues in organisations. The chapter began by firstly outlining the research design followed. Next, the research method was discussed and finally, the findings were presented and analysed. This was done to confirm if what is taught at leading universities in the field is reflected practically in the approach taken by organisations. Additionally, it was also done to highlight some further considerations that may be of relevance to the discussions around modelling knowledge security. With the completed empirical component and previous theory discussed in the dissertation acting as a foundation, Chapter 7 will commence with a discussion around how knowledge security can be modelled as a KM problem conceptually. This will form the final section of the research related to conceptual model development, with the objective being to examine how knowledge security can be modelled conceptually as a KM problem and be presented as a model.

⁹²⁴ Research sub-question 6.1: *Does what is done in practice reflect the elements found in academic teaching?*

⁹²⁵ Research sub-question 6.2: *What is the relationship between KM and security in practice?*

Part 3 – Conceptual Model

Chapter 7

Modelling Knowledge Security as a Knowledge Management Problem

7.1 Introduction

Chapter 7 forms the final part of the research and discusses the process of conceptualising knowledge security as a KM problem, presenting it as a model. Thus, the chapter begins by selecting a conceptual modelling approach, through an examination of how conceptual modelling has been applied to KM. A conceptual modelling approach is then compiled from the array of modelling approach factors identified. In addition, a brief examination of the literature is done relating to other conceptual models of knowledge security. This is necessary as several models of knowledge security have emerged in recent years since this project began. Apart from keeping up to date with developments in the literature, these models may provide additional insights and inputs for the development of my model. Next, the process of developing the conceptual model is outlined and discussed, as derived from the compiled modelling approach, and relevant actions are taken. Following this, the limitations of the model are briefly discussed and ideas for future research are presented.

7.2 Selecting a Conceptual Modelling Approach

To establish this approach, I firstly provide an overview of what conceptual modelling is and how it is used, including those aspects that are important to follow concerning developing a conceptual model. I aim to link this back to my proposed approach presented in this dissertation. Secondly, I examine what conceptual models can be found in the literature, relating to knowledge security, to determine a base of existing research and to help provide any further inputs relating to the development of the conceptual model. Thirdly, I integrate these aspects and present the process that I followed to develop and document my conceptual model of knowledge security. Doing so provides a framework for the discussion to follow, expanded upon in the remaining sections of this chapter.

7.2.1 Brief Overview of Conceptual Modelling

From within the broader construct of scientific modelling⁹²⁶, which aims to understand, define, quantify, visualise, or simulate something through references to commonly accepted knowledge⁹²⁷, conceptual modelling has been applied to and used in a variety of fields⁹²⁸. Examples of this application include computer science⁹²⁹, information systems, software design, database design⁹³⁰, simulations⁹³¹, product design⁹³², information security⁹³³, business process engineering⁹³⁴, KM⁹³⁵ and many other fields. In each field, variations in approaches taken can be observed depending on the context in which it is used and the objectives of that field.

In its most basic form, conceptual modelling often follows a system focus with Dragicevic *et al.* defining it as a “simplified representation of a target system”⁹³⁶. From this view, it is seen as independent of design or implementation concerns⁹³⁷ and may be based on a mathematical⁹³⁸ or non-mathematical approach⁹³⁹, depending on the objective of the model. Thalheim states that while there is a technological and scientific component to conceptual modelling, depending on the field, its success also depends on understanding the environment through “comparatively sophisticated skills of literacy and numeracy”⁹⁴⁰. Thalheim further states that “at the same time, modelling is an art. Modelling is a highly creative process”⁹⁴¹. Through this simplified

⁹²⁶ Hacking & Hacking, 1983. *Representing and Intervening. Introductory Topics in the Philosophy of Natural Science*.

⁹²⁷ Wikipedia, 2021. *Scientific Modelling* [Online].

⁹²⁸ Wikipedia, 2021. *Scientific Modelling* [Online].

⁹²⁹ Science Direct, 2021. *Conceptual Model* [Online].

⁹³⁰ Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1669.

⁹³¹ Balci & Ormsby, 2007. *Conceptual Modelling for Designing Large-Scale Simulations* p 175-186.

⁹³² Beju *et al.*, 2013. *A Conceptual Model of Product Design* p 908-912.

⁹³³ Bharathi & Suguna, 2014. *A Conceptual Model to Understand Information Security Awareness* p 402-405.

⁹³⁴ Robinson & Arbez, 2015. *Conceptual Modelling: Definition, Purpose and Benefits* p 2822.

⁹³⁵ Karagiannis *et al.*, 2017. *How can Diagrammatic Conceptual Modelling Support Knowledge Management?* p 1-18.

⁹³⁶ Dragicevic *et al.*, 2020. *A Conceptual Model of Knowledge Dynamics in the Industry 4.0 Smart Grid Scenario* p 208.

⁹³⁷ Definitions.net, 2021. *Definitions for Conceptual Model* [Online].

⁹³⁸ Singleton & Straits, 2010. *Approaches to Social Research* p 537.

⁹³⁹ Morgan, 2005. *Basic Guidance for Cross-Cutting Tools: Conceptual Models. Guidance for Conceptual Models* p 1.

⁹⁴⁰ Thalheim, 2012. *The Science and Art of Conceptual Modelling* p 76-105.

⁹⁴¹ Thalheim, 2012. *The Science and Art of Conceptual Modelling* p 76-105.

representation, conceptual models can be used to describe the nature of a concept⁹⁴² or series of concepts and the key activities that are encompassed therein⁹⁴³. This includes the relationships between the concepts, providing a framework in the organisational sense, of the knowledge of a particular discipline or to determine its focus⁹⁴⁴. It thus serves as a guide for observation and interpretation that can deepen understanding, which may include aspects of the physical or social world⁹⁴⁵. In some instances, it can also be used to simulate the subject of that model⁹⁴⁶. Within a conceptual model, the relationship between the collection of concepts can also be represented graphically. Heemskerk *et al.* state that this “is typically drawn as a series of diagrams with boxes and arrows that show the main elements and flows of material, information and causation that define a system”⁹⁴⁷.

Thalheim⁹⁴⁸ explains that conceptual models are in essence schematic descriptions of a system, a theory, or a phenomenon of an origin that form a model. According to Thalheim⁹⁴⁹, their development requires planning, making, or executing through a deep insight into the background area as well as skills, simplification, experience, and ingenuity. Further, while each field will have its own culture or approach to modelling, this is often learned and shared within communities⁹⁵⁰. Thalheim⁹⁵¹ argues that each community will have its own approach, thus making modelling a non-formalised approach, in that communities heuristically use operational and scientific terms. This view is also supported by Brooks and Wang⁹⁵², whereby they state that “it is unrealistic to expect one set of guidelines or one method to apply to all applications” of conceptual modelling. Rather, Brooks and Wang⁹⁵³ explain that it is best to find a compatible approach for specific domains as required.

⁹⁴² Gregory, 1993. *Cause, Effect, Efficiency & Soft Systems Models* p 333-344.

⁹⁴³ Ale *et al.*, 2005. *A Distributed Knowledge Management Conceptual Model for Knowledge Organizations* p 1-14.

⁹⁴⁴ Miller & Keane, 1983. *Encyclopaedia and Dictionary of Medicine, Nursing and Allied Health*.

⁹⁴⁵ Mylopoulos, 1992. *Conceptual Modelling, Databases, and Case - An Integrated View of Information Systems Development* p 49-68.

⁹⁴⁶ Wood, 2016. *Conceptual Models: Definitions and Characteristics* [Online].

⁹⁴⁷ Heemskerk *et al.*, 2003. *Conceptual Models as Tools for Communication Across Disciplines*.

⁹⁴⁸ Thalheim, 2012. *The Science and Art of Conceptual Modelling* p 76-105.

⁹⁴⁹ Thalheim, 2012. *The Science and Art of Conceptual Modelling* p 76-105.

⁹⁵⁰ Thalheim, 2012. *The Science and Art of Conceptual Modelling* p 76-105.

⁹⁵¹ Thalheim, 2012. *The Science and Art of Conceptual Modelling* p 76-105.

⁹⁵² Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1672.

⁹⁵³ Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1672.

7.2.2 Conceptual Modelling as Applied to Knowledge Management

In line with this discussion, as there appears not to be one formalised approach across fields due to variance amongst subject domains⁹⁵⁴, it becomes important to select an approach that is relevant to a KM perspective. Therefore, to better evaluate how conceptual modelling is applied in KM, from a methodological standpoint, I chose to summarise a random sample of KM modelling approaches used. The approaches were outlined in 10 articles selected through a brief examination of the literature and covered 12 years. Once the articles had been identified, I proceeded to read through each of the articles and summarise the processes followed through their various sections. The conceptual modelling approaches that I identified through this process were then compiled from a high-level view as presented in Table 7-14.

Next, to identify the most common steps, I used spreadsheet software to analyse the approach summaries from Table 7-14, looking for commonalities amongst the terms used. To do this, I consolidated and then counted the number of times each of the steps were mentioned in Table 7-14. I also did this to help ensure that whatever process I chose to follow would account for the most important elements used when developing conceptual models from a KM perspective. The key steps identified and their listed popularity as analysed, not in order of appearance, are presented in Table 7-15.

7.2.3 Choosing an Approach to Conceptual Modelling

According to Kotiadis *et al.*⁹⁵⁵, in developing a conceptual model, the modeller needs to decide what to model and how to model it. This is done to create a justifiable representation of the system being modelled. Therefore, since choosing an approach to developing a conceptual model needs to be relevant to my objectives while aligning with the standards of the community⁹⁵⁶, I chose to adopt those steps from Table 7-15 as deemed appropriate to my needs. In my view, this is a justifiable approach to take for two reasons. Firstly, in doing so it positions my conceptual model within the broader domain of KM approaches to conceptual modelling. Secondly, as not every researcher outlined in Table 7-14 uses every step but rather those relevant to their objectives, choosing those steps applicable to my needs is also justifiable.

⁹⁵⁴ Thalheim, 2012. *The Science and Art of Conceptual Modelling* p 76-105.

⁹⁵⁵ Kotiadis *et al.*, 2014. *A Participative and Facilitative Conceptual Modelling Framework for Discrete Event Simulation Studies in Healthcare* p 197-213.

⁹⁵⁶ Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1672.

Table 7-14: Examples of Conceptual Modelling Approaches in KM

Overview	Summary of Approach
<p>Authors: Dragicevic <i>et al.</i>⁹⁵⁷ (2020)</p> <p>General KM Area – Knowledge Dynamics</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Extract required inputs related to objectives 4. Use inputs to construct model 5. Discuss model and implications
<p>Authors: Helmy <i>et al.</i>⁹⁵⁸ (2020)</p> <p>General KM Area – Social Business Processes</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Identify gaps in the literature 4. Establish concepts 5. Integrate concepts into model 6. Discuss model and implications
<p>Authors: Elliott <i>et al.</i>⁹⁵⁹ (2019)</p> <p>General KM Area – Knowledge Security</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Extract required inputs related to objectives 4. Use inputs to construct model 5. Discuss and describe inputs 6. Conduct case study for further understanding 7. Discuss model and implications
<p>Authors: Farooq⁹⁶⁰ (2019)</p> <p>General KM Area – Value Creation</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Identify gaps in the literature 4. Establish concepts 5. Integrate concepts into model 6. Discuss model and implications

⁹⁵⁷ Dragicevic *et al.*, 2020. *A Conceptual Model of Knowledge Dynamics in the Industry 4.0 Smart Grid Scenario* p 208.

⁹⁵⁸ Helmy *et al.*, 2020. *A Conceptual Ontological Framework for Managing the Social Business Process to Enhance Customer Experience* p 262-271.

⁹⁵⁹ Elliott *et al.*, 2019. *Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs* p 179-193.

⁹⁶⁰ Farooq, 2019. *Developing a Conceptual Framework of Knowledge Management* p 139.

Overview	Summary of Approach
<p>Authors: Ilvonen⁹⁶¹ (2016)</p> <p>General KM Area – Knowledge Security</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Establish concepts and present model 4. Discuss concepts of model 5. Provide illustrative case study 6. Discuss model and implications
<p>Authors: Pennington⁹⁶² (2016)</p> <p>General KM Area – Knowledge Integration</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Synthesise current research 4. Identify core concepts and inputs 5. Integrate concepts into model 6. Discuss model and implications
<p>Authors: Waheed & Kaur⁹⁶³ (2014)</p> <p>General KM Area – Knowledge Quality</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Identify gaps in the literature 4. Synthesise current research and models 5. Identify core concepts and inputs 6. Integrate concepts into models 7. Discuss concepts of models
<p>Authors: Sedighi & Zand⁹⁶⁴ (2012)</p> <p>General KM Area – Critical Success Factors</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Establish concepts and integrate into a model 3. Discuss concepts of model 4. Discuss model and implications

⁹⁶¹ Ilvonen *et al.*, 2016. *Towards a Business-Driven Process Model for Knowledge Security Risk Management: Making Sense of Knowledge Risks* p 1-18.

⁹⁶² Pennington, 2016. *A Conceptual Model for Knowledge Integration in Interdisciplinary Teams: Orchestrating Individual Learning and Group Processes* p 300-312.

⁹⁶³ Waheed & Kaur, 2014. *Knowledge Quality: A Review and a Revised Conceptual Model* p 1-15.

⁹⁶⁴ Sedighi & Zand, 2012. *Knowledge Management: Review of the Critical Success Factors and Development of a Conceptual Classification Model* p 1-9.

Overview	Summary of Approach
<p>Authors: Bhatti <i>et al.</i>⁹⁶⁵ (2011)</p> <p>General KM Area – Innovation and Performance</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Identify gaps in the literature 4. Outline contribution of research 5. Identify core concepts and inputs 6. Integrate concepts into a model
<p>Authors: Zanjani <i>et al.</i>⁹⁶⁶ (2008)</p> <p>General KM Area – Customer KM</p>	<ol style="list-style-type: none"> 1. Outline problem and objectives 2. Review literature 3. Identify core concepts and inputs 4. Discuss core concepts and inputs 5. Integrate concepts into a model 6. Provide illustrative case study

Table 7-15: Summary of KM Conceptual Modelling Steps and their Popularity

Element	Appearance in Articles Reviewed
Outline problem and objectives	10
Review literature	9
Identify gaps in literature/contribution	5
Synthesise current research	2
Identify/establish core concepts/inputs	10
Integrate inputs/concepts into a model	10
Discuss/describe concepts/inputs of model	5
Discuss model and implications	7
Provide illustrative case study	3

⁹⁶⁵ Bhatti *et al.*, 2011. *The Effect of Knowledge Management Practices on Organisational Performance: A Conceptual Study* p 2847-2853.

⁹⁶⁶ Zanjani *et al.*, 2008. *Proposing a Conceptual Model of Customer Knowledge Management: A Study of CKM Tools in British Dotcoms* p 303-307.

It should thus be noted that not all the broader KM modelling steps listed in Table 7-15, as related to each of my steps, will be applicable. Thus, the steps that I have chosen to follow, in line with my broader research objectives, have been summarised in Table 7-16. I have also indicated their general relationship to the broader KM modelling elements as shown in Table 7-15 to add context.

Table 7-16: My Selected Conceptual Modelling Approach in Relation to KM Modelling Steps

My Selected Approach	Relationship to Broader KM Modelling Steps
1.) Establish the objectives of the model	Outline problem and objectives (10)
2.) Review sources of information	Review literature (9) Identify gaps in literature/contribution (5) Synthesise current research (2)
3.) Extract relevant model inputs from the reviewed sources of information	Identify/establish core concepts/inputs (10)
4.) Integrate relevant model inputs into a model	Integrate inputs/concepts into a model (10)
5.) Discuss the model and implications	Discuss/describe concepts/inputs of model (5) Discuss model and implications (7)
	Provide illustrative case study (3)

As can be seen in Table 7-16, most of my steps relate to the broader KM modelling elements as shown in Table 7-15. The only element that is not covered by my approach is that of providing an illustrative case study. While this would have been useful to include, it is beyond the current scope of this research, which is focused on laying the framework for the development of the conceptual model. Additionally, as shown from the process examples provided in Table 7-14, it is also not a component that is included in the first phase of all conceptual modelling research in KM. A further point to note is that while each of the steps of my chosen approach is presented sequentially, some aspects in practice are handled iteratively,

as a certain degree of reworking and remodelling is required. I will now briefly outline each of the steps in Table 7-16 concerning my objectives and how I will proceed going forward. The steps outlined below will be discussed and expanded upon in Section 7.3 and form the sub-sections of that discussion.

- **Step 1: Establish the objectives of the model** – This step will outline the objective of the model in the context of the broader research objectives of the dissertation.
- **Step 2: Review sources of information** – This step will outline the different sources of information that will need to be reviewed to derive the inputs for the model.
- **Step 3: Extract relevant model inputs from the reviewed sources of information** – This step will list and discuss the identified elements from the chosen sources of information that will be integrated to form the model.
- **Step 4: Integrate relevant model inputs into a model** – This step will integrate the various identified inputs and represent them graphically as a conceptual model.
- **Step 5: Discuss the model and implications** – This step will discuss the fit and relationship of the integrated inputs in the model and provide more details relating to each component of the model. The implications of combining the various inputs in the model will also be discussed.

Finally, before proceeding to the discussion in Section 7.3, one aspect that needs to be updated from the literature is the published research on existing models of knowledge security. While conceptual models of knowledge security were not present at the start of this dissertation process, several have emerged in the literature in recent years. I decided that it is important to include these here for two reasons. Firstly, they inform the discussion and development of my model as they may illuminate different approaches to developing a conceptual model of knowledge security or highlight different aspects of importance to focus on. Secondly, they may also provide useful insights and further inputs that can be used in the development of my conceptual model. This may be in the form of separate approaches, or whereby I may be able to relate their research to that of my model, thus more effectively covering the topic and in turn remaining better up to date with developments in the literature.

7.2.4 Overview of Conceptual Models in Knowledge Security

As mentioned, conceptual modelling has also been used to conceptualise knowledge security issues related to KM but less prolifically. Thus, while conducting a literature search for examples of conceptual models focusing on knowledge security, only a few examples could be

found. I will briefly outline these models in the paragraphs to follow to determine a base of existing research and to help provide any further inputs relating to the development of the conceptual model.

To begin, Ilvonen conducted, for her doctoral research, a conceptual analysis of knowledge security⁹⁶⁷. Ilvonen examined how the concept of information security management, framed to meet the requirements of the CIA triad, could be extended to encompass KM activities too. Ilvonen did this by aiming to determine what knowledge security means, by developing an integrated view of information security management and KM activities and their overlap. These two domains were then combined as an integrated concept, that of knowledge security and presented as a model. Ilvonen's approach also consisted of a theoretical analysis and an empirical component which were used to provide inputs for the synthesis processes. Ilvonen concluded her analysis by stating that, in her view, "knowledge security is a process aimed at the security of knowledge that is embedded in the people working for a company and in their interactions"⁹⁶⁸. Ilvonen⁹⁶⁹ suggests that it is important for an organisation to be able to identify the threats to knowledge and for KM initiatives to be examined in a coherent form.

In a subsequent publication, Ilvonen *et al.* also highlighted the importance of knowledge security risk management as a factor in contemporary organisations⁹⁷⁰. They outline that knowledge security risk management should be developed toward a more proactive management of the potential future risks of knowledge sharing⁹⁷¹. They explain that this is important as the environment is more dynamic than traditional information security management models⁹⁷². Thus, they propose a model for knowledge security risk management (KSRM) consisting of the process elements of: 1) Business need or problem and expected benefits from change, 2) Knowledge identification, 3) Threat identification, 4) Risk analysis, 5) Cost/benefit assessment, 6) Mitigation and 7) Monitoring⁹⁷³. By following the approach

⁹⁶⁷ Ilvonen, 2013. *Knowledge Security - A Conceptual Analysis* p 1-172.

⁹⁶⁸ Ilvonen, 2013. *Knowledge Security - A Conceptual Analysis* p 1-172.

⁹⁶⁹ Ilvonen, 2013. *Knowledge Security - A Conceptual Analysis* p i.

⁹⁷⁰ Ilvonen *et al.*, 2015. *Knowledge Security Risk Management in Contemporary Companies - Toward a Proactive Approach* p 3941.

⁹⁷¹ Ilvonen *et al.*, 2015. *Knowledge Security Risk Management in Contemporary Companies - Toward a Proactive Approach* p 3941.

⁹⁷² Ilvonen *et al.*, 2015. *Knowledge Security Risk Management in Contemporary Companies - Toward a Proactive Approach* p 3941.

⁹⁷³ Ilvonen *et al.*, 2015. *Knowledge Security Risk Management in Contemporary Companies - Toward a Proactive Approach* p 3944-3947.

outlined in the KSRM, they argue that it provides a useful approach to evaluate what knowledge is important, how it should be shared and what should be considered when securing it⁹⁷⁴. As a further refinement to their KSRM model, Ilvonen *et al.* expanded their approach in an additional research paper, whereby they highlighted the importance of sense-making⁹⁷⁵ as a mechanism for adding context. They did this to improve the KSRM process by helping the organisation to understand its business situation, environment, and appropriate knowledge⁹⁷⁶. By highlighting this aspect, Ilvonen *et al.* explain that it also helps to describe the business case of the intended change and what kind of benefits are sought by implementing that change⁹⁷⁷.

Next, Elliott *et al.* propose a conceptual framework that examines the organisational methods of knowledge protection, whose objective is to strike a balance between sharing and protection⁹⁷⁸. The framework highlights the benefits of sharing and risks, as moderated by several factors within the context of intra- and inter-organisational sharing. These factors, Elliott *et al.* argue affect the procedures that organisations implement to govern their knowledge protection and sharing processes⁹⁷⁹. Elliott *et al.* state that through the framework a basic trade-off is highlighted between “improving decision-making and innovation through communication and mitigating security risks by imposing restrictions on communication flows”⁹⁸⁰. The mediating factors are the sensitivity of the information, the degree to which employees can be trusted with such information and the firm’s level of legal protection mechanisms⁹⁸¹. An important factor that Elliott *et al.* highlight is the context in which such sharing takes place, which can influence the cost-benefit analysis of information restrictions⁹⁸².

⁹⁷⁴ Ilvonen *et al.*, 2015. *Knowledge Security Risk Management in Contemporary Companies - Toward a Proactive Approach* p 3948.

⁹⁷⁵ Ilvonen *et al.*, 2016. *Towards a Business-Driven Process Model for Knowledge Security Risk Management: Making Sense of Knowledge Risks* p 4-7.

⁹⁷⁶ Ilvonen *et al.*, 2016. *Towards a Business-Driven Process Model for Knowledge Security Risk Management: Making Sense of Knowledge Risks* p 4-7.

⁹⁷⁷ Ilvonen *et al.*, 2016. *Towards a Business-Driven Process Model for Knowledge Security Risk Management: Making Sense of Knowledge Risks* p 4-7.

⁹⁷⁸ Elliott *et al.*, 2019. *Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs* p 182.

⁹⁷⁹ Elliott *et al.*, 2019. *Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs* p 182.

⁹⁸⁰ Elliott *et al.*, 2019. *Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs* p 179.

⁹⁸¹ Elliott *et al.*, 2019. *Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs* p 179-183.

⁹⁸² Elliott *et al.*, 2019. *Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs* p 179-183.

They note that the knowledge sharing risk within an organisation as opposed to external sharing with partners, suppliers and customers is lower. In this regard, Elliott *et al.* view sharing information externally as more hazardous as it can be a risk to the firm's distinctive competencies⁹⁸³.

7.3 Developing a Conceptual Model of Knowledge Security

With my modelling approach acting as a guide, as outlined in Table 7-16, I proceeded to work through each of the various steps in more detail. Through this process, and the discussions in each of the sections, my conceptual model of knowledge security was developed. Each of these elements is discussed in greater detail in the sub-sections to follow. This is in terms of establishing the objectives of the model, reviewing sources of information, extracting relevant model inputs, integrating relevant inputs into a model, and discussing it and its implications.

7.3.1 Establishing the Objectives of the Model

In terms of the objectives of the model, it aligns broadly with the primary research objective of the dissertation. The primary research objective is focused on developing a conceptual modelling approach that will help conceptualise knowledge security as a KM problem. Practically, this means creating a simplified representation that integrates the different dimensions of KM with those of knowledge security. The model thus acts as a representative framework to increase understanding through alleviating the unclear relationships between the concepts. In providing a theoretical structure, it also creates a base framework upon which further research can be built or tested.

7.3.2 Reviewing Sources of Information

The sources of information that I reviewed consisted of the theoretical and empirical elements presented in the previous chapters of this dissertation. From the theoretical perspective, this related to the topics discussed around the composition of possible KM solutions and activities (Chapter 1), defining organisational knowledge (Chapter 2), defining knowledge management and the need for an integrated approach to security (Chapter 3), the literature review of knowledge security approaches (Chapter 4) and any other elements illuminated through the discussion of modelling knowledge security as a KM problem (Chapter 7). From the empirical

⁹⁸³ Elliott *et al.*, 2019. *Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs* p 183.

perspective, this related to the practical outcomes investigated around the review of knowledge security in leading academic programs (Chapter 5) and the interview discussions related to KM and knowledge security in practice (Chapter 6).

7.3.3 Extracting Relevant Model Inputs

In this section, I list and discuss any identified elements as chosen from the identified sources of information. The focus is on examining the objective outcomes of the listed sources of information, in this case, the various chapters of this dissertation, and then choosing what was regarded as the most relevant inputs for my model. It is important to note that as part of this process, there was some overlap in the identification of the inputs derived from each of the chapters. However, where possible, any such overlaps were consolidated and refined before inclusion into the final version of the model. I also considered some additional elements from the chapters, where relevant, but these were not my primary focus. As the arguments and justifications have been explained in those individual chapters, for the development of the various inputs, I chose not to discuss them again here. Rather, focus was given to their relevance in the context of the development of the model and to what they can contribute. The inputs derived from the analysis of the chapters are summarised in Table 7-17.

7.3.3.1 Chapter 1 – Discussion and Inputs

As part of the introductory discussion in the chapter, the need for knowledge security to be aligned with KM activity was examined. Part of this discussion focused on the view of KM solutions put forward by Becerra-Fernandez and Sabherwal⁹⁸⁴, whereby they developed a consolidated framework of KM activities that can be found in organisations. The framework outlines intra-organisational KM activity made up of processes, systems, mechanisms, technologies, and infrastructure.

From the perspective of model development, this framework can be used as a comprehensive representation of KM activity. It also acts as a practical tool to identify those dimensions where knowledge security issues will be found within the broader realm of KM. The collection of KM solutions frames which relevant KM governance activities are applied. From a knowledge security perspective, the collection of KM solutions frames how knowledge security risk can be assessed and controls implemented in the context of the organisation and its requirements.

⁹⁸⁴ As referenced in Section 1.1, paragraph 9.

Table 7-17: Summary of Model Inputs Derived from the Analysis of the Chapters

Chapter	Primary Objectives	Inputs Derived from Analysis
Chapter 1	<ul style="list-style-type: none"> Introductory concepts and discussion 	<ul style="list-style-type: none"> KM solutions, as per Becerra-Fernandez and Sabherwal's view of KM activities in organisations
Chapter 2	<ul style="list-style-type: none"> Define organisational knowledge through an analysis of the literature 	<ul style="list-style-type: none"> Context, as per Tsoukas's definition of knowledge
Chapter 3	<ul style="list-style-type: none"> Define KM through an analysis of the key views from the literature Examine the need for an integrated approach between security and KM 	<ul style="list-style-type: none"> Context with the addition of strategic focus Alignment between information security, knowledge security and KM
Chapter 4	<ul style="list-style-type: none"> A literature review of current approaches to knowledge security while keeping the KM paradigm in mind 	<ul style="list-style-type: none"> Technical and non-technical knowledge security paradigms, with an emphasis on risk management elements
Chapter 5	<ul style="list-style-type: none"> Review of knowledge security in leading academic programs in the EUR and USA as part of the investigation into knowledge security To determine if knowledge and security are treated as separate entities 	<ul style="list-style-type: none"> Intellectual property protection mechanisms Employee knowledge retention mechanisms Information protection mechanisms
Chapter 6	<ul style="list-style-type: none"> Discuss the results of a series of case study interviews done with leading experts in relation to the findings presented in Chapter 5 Obtain a practical view of the relationship between knowledge and security in organisations 	<ul style="list-style-type: none"> Risk management Information security elements Knowledge security controls Balance between KM solutions and culture Balance between security and KM objectives Knowledge value considerations
Chapter 7	<ul style="list-style-type: none"> Developing a conceptual model of knowledge security 	<ul style="list-style-type: none"> Alignment between information security and KM Importance of risk Importance of context in the determination of value and acceptable levels of sharing

The collection of KM solutions also forms a focal point for the intersection of KM governance and knowledge security activities in practice. Thus, the input of KM solutions as per Becerra-Fernandez and Sabherwal's view of KM activities in organisations is seen as important.

7.3.3.2 Chapter 2 – Discussion and Inputs

The objective of the chapter was to define organisational knowledge through an analysis of the literature. Through this process, I chose to adopt the definition offered by Tsoukas⁹⁸⁵ consisting of two forms: the weak and strong views of organisational knowledge. I made this choice due to the definition's ability to frame key organisational knowledge issues of the context and environment, social aspects, and knowledge transfer from a deeper theoretical perspective. The deeper theoretical perspective is enabled by Tsouka's emphasis on the tacit and explicit relationship and how it manifests in organisations as distributed knowledge systems. To recap, from the weak view, Tsoukas and Vladimirou define organisational knowledge simply as being generated, developed, and transmitted by individuals, which as they claim is less revealing about the deeper characteristics of what organisational knowledge is. From the strong view, Tsoukas and Vladimirou define organisational knowledge as emerging when individuals within organisations consider the context of their actions. These individuals do so by drawing upon and acting upon a corpus of generalisations that are produced internally because of organisational processes and tasks.

The important aspect of this definition, in the scope of developing a conceptual model of knowledge security, is that it highlights the importance of context in the way organisations view and manage their knowledge. By doing so, it helps to emphasise the processes, socialisation elements and intersections of interests rather than the individual KM mechanisms alone. If framed in this way, knowledge can be seen to be dependent on context and meaning derived by those using it within the context of an organisation. At the same time, it can be seen to be feeding back to what is viewed and applied as knowledge in that context. From a knowledge security perspective, this is important as without context it is not clear as to what knowledge is of value to an organisation and where that value lies. Further, context will have implications for the way knowledge is governed by KM. It will also have implications for the way it is applied to KM solution areas such as processes, systems, mechanisms, technologies, and infrastructure within an organisation⁹⁸⁶. How this is framed by the said context will then

⁹⁸⁵ As and referenced in Section 2.2.3, paragraphs 23-26; Section 2.2.4, paragraph 7; Section 2.3.

⁹⁸⁶ As referenced in Section 1.1, paragraph 9.

also determine where knowledge security risks may be found. It can also help to determine in what areas of these KM solutions they may be most prominent. Thus, the input of context as per Tsoukas's definition of knowledge is seen as important.

7.3.3.3 Chapter 3 – Discussion and Inputs

There were two main objectives of the chapter. These were to define KM through an analysis of the key views from the literature and to examine the need for an integrated approach between security and KM. Firstly, in terms of defining KM, I chose to adopt Girard and Girard's integrated definition whereby they define KM as "the management process of creating, sharing and using organisational information and knowledge"⁹⁸⁷. I did this due to the definition's ability to highlight the management process aspect of KM as opposed to a purely process-orientated view. It in turn relates to Becerra-Fernandez and Sabherwal's KM framework in that they highlight the importance of KM processes which will be important to any security approach. The definition also highlights the different ages, phases, or generations⁹⁸⁸ that KM may take in an organisation and whether knowledge in that context is seen as a resource or a capability⁹⁸⁹. Using KM as a capability allows an organisation to adapt strategically to the needs of its environment by using its collective knowledge. The different approaches to KM will thus have different security implications too. This is an important aspect from the perspective of model development, as it reaffirms the importance of context. It also emphasises the strategic focus that an organisation has as to their KM needs and how that is applied in practice. From a knowledge security perspective, it again becomes important to keep the context and strategic focus of any KM initiative in mind. Thus, the input of context with the addition of strategic focus is seen as important in this regard.

Secondly, concerning the need for an integrated approach between security and KM, and the need for knowledge security, several factors were discussed. These factors relate to the difference between information and knowledge and how these differences translate to different requirements for managing and securing them. For example, as discussed in the chapter, IM takes a more resource-based view, focused on managing information in electronic or physical

⁹⁸⁷ As referenced in Section 3.5. paragraph 5.

⁹⁸⁸ This in terms of the views put forward by Snowden (structuring and flow of information, SECI model, systemic flow view), Davenport and Cronin (information management, business process contextualisation, knowledge as a capability) and Tuomi (clustering of approaches, centralised sharing, collective social understanding).

⁹⁸⁹ As referenced in Section 3.3. paragraphs 22-26; Section 3.4, paragraph 1.

forms⁹⁹⁰. This differs from KM, which can take both a resource-based view (the handling of knowledge in a KMS), while also extending to a capability-based view requiring further social, sense-making and decision-making processes. This difference highlights the degree of social interaction needed in the management of knowledge as opposed to information. As with KM, people are often at the core of creating and processing knowledge⁹⁹¹. It thus relies on deduction, socialisation processes, understanding and the interplay between individuals in a particular context. These are important perspectives and both aspects would need to be catered for in any approach to securing an organisation's knowledge that is aligned with KM.

In terms of model development, this is also important for two reasons. Firstly, to ensure that both the technical resource elements are protected in addition to the broader non-tangible strategic and socialisation aspects. Secondly, to ensure that both aspects of information security and knowledge security mechanisms are aligned with KM practices and tasks, to know what to focus on. Jennex and Durcikova⁹⁹² suggest that information systems security and KM should be viewed as complementary activities. From a knowledge security perspective, these inputs are important as they highlight the need for an approach that accounts for the broader contextual and strategic dynamics of KM. Yet, an approach that also acts as a conduit to better align information security practices and knowledge security practices with KM, as per their contextual and strategic objectives. Thus, the input of the alignment between information security, knowledge security and KM should be viewed as important in this regard.

7.3.3.4 Chapter 4 – Discussion and Inputs

The chapter focused on conducting a literature review of current approaches to knowledge security while keeping the KM paradigm in mind. Several knowledge security paradigms were identified and categorised according to various perspectives presented within each paradigm. It was found that there is a clear research focus orientated towards approaches related to systems security (18 texts), assurance (11 texts), risk management (7 texts), and DIS (2 texts). The balance of this focus appears to be aligned with the growth in the importance of information security elements and their inevitable application to aspects of KM, as discussed in Chapter 4. As such, there is a substantial focus on knowledge security approaches dealing with technical factors. To a lesser degree, there is also a focus on management issues aimed at

⁹⁹⁰ As referenced in Section 4.2, paragraph 7.

⁹⁹¹ Yadav & Singh, 2013. *A role of knowledge management in organizational performance* p 195-201.

⁹⁹² Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat?* p 3452.

mitigating the complexity of securing knowledge in KMSs as opposed to traditional information systems⁹⁹³. An important point, concerning this second aspect, is the focus on assurance and risk management issues. From a practical perspective, there is a need for more alignment with business policy, processes, privacy issues and knowledge security policy⁹⁹⁴. Thus, this perspective indicates a need for approaches focused on both technical and non-technical security issues. It is also important to consider the DIS perspectives. These are based on counterintelligence principles and have the potential to mitigate many of the less tangible threats targeted towards organisational knowledge, such as intelligence gathering.

From a perspective of model development, it will be important to represent both these technical elements and non-technical paradigms and perspectives. Additionally, the paradigms related to knowledge security risk management will be important, as they contribute to determining the application of security mechanisms and controls relevant to a particular context. Risk evaluation will also help in this regard, by identifying what knowledge is of value to a particular organisation.

From a knowledge security perspective, focusing on technical and non-technical elements will enrich the security controls available and provide a link to relevant information security elements from within the broader knowledge security focus. It will also help shape how these elements can be related to the KM objectives of an organisation to determine what security controls would be needed from a risk perspective. This would be framed by the organisational context and focus regarding knowledge and KM as applied through relevant KM solutions. An added benefit of this approach is that it would also help to determine the right balance between sharing and protecting knowledge from a strategic perspective. The balance between the two would be governed by the determination of the value that the knowledge holds for the organisation, as opposed to the relevant level of determining risk. Therefore, it would follow a risk to benefit trade-off, possibly actualised through security models such as the CIA triad and would apply to each organisation's particular set of needs. Thus, the input of technical and non-technical knowledge security paradigms, with an emphasis on risk management elements will be important in this regard.

⁹⁹³ As referenced in Section 4.3.3.5, paragraph 4.

⁹⁹⁴ Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p 425.

7.3.3.5 Chapter 5 – Discussion and Inputs

The focus of the chapter was to review knowledge security in leading academic programs in the EUR and USA as part of the investigation into knowledge security. The purpose was to see if knowledge and security are treated as separate entities and to provide additional inputs for the development of the conceptual model. It was found that while there was some mention of security and knowledge in certain academic programs, most had a broader focus on related concepts. These concepts included IP protection mechanisms (legal), employee knowledge retention mechanisms (employee retention, archiving the explicit, and transferring the tacit) and information protection mechanisms (information security, governance, risk, and compliance).

Firstly, in terms of IP protection mechanisms, the focus was predominantly centred on legal elements applied to things like IT systems, leadership, international business development, economic, and engineering considerations. Practically, examples of these legal elements include patents, copyrights, NDAs and so forth. Secondly, in terms of employee knowledge retention mechanisms, it was generally framed from a knowledge governance or HR perspective. The purpose of doing so was to retain key individuals and thus their knowledge and skills. Practically, this was actualised through elements such as retaining highly skilled people within an organisation with appropriate benefits, having processes in place to archive knowledge in systems and being able to capture or transfer the knowledge of key employees who might leave. Thirdly, in terms of information protection mechanisms, in some instances, concepts from information security were linked to the topic through IM. This manifested in situations where it was taught in conjunction with KM, focused largely on information systems, and as applied to KM technologies too. There was also a general link to security being important for KM, as framed from within the broader objectives of organisational information governance, risk and compliance.

From the perspective of model development, the security concepts highlighted above will be important. Their importance is in terms of forming part of the list of the broader knowledge protection elements available. This relates to the inclusion of both IP protection mechanisms and employee knowledge retention mechanisms. These elements form part of the set of knowledge protection elements available within the broader knowledge security approach. The focus on information protection mechanisms also highlights the importance of having a link between KM, knowledge security and information security objectives. The purpose is to form part of the broader organisational governance and risk strategy of the organisation.

From a knowledge security perspective, the combination of these mechanisms will help to provide a more comprehensive list of possible knowledge and information security controls. These controls are framed from within the broader framework of the knowledge security approach taken. Relevant controls can thus be determined and applied through the inclusion of knowledge security risk management processes. The application of these controls will then be relevant to the various KM solutions that have been implemented. They will also be dependent on the defined context of the organisation and will form part of the organisation's broader strategic governance objectives. Thus, the inputs of IP protection mechanisms, employee knowledge retention mechanisms and information protection mechanisms will be important in this regard.

7.3.3.6 Chapter 6 – Discussion and Inputs

The focus of the chapter was to discuss the results of a series of case study interviews done with leading experts related to the findings presented in Chapter 5. The purpose of doing so was to obtain a practical view of the relationship between knowledge and security in organisations and to garner any additional inputs for the conceptual model that might be of importance. In terms of the importance of the findings concerning Chapter 5, there was a strong focus on governance, risk, and compliance (100%), knowledge security from an information security perspective (87.5%), and the archiving of explicit knowledge in systems (75%). There was a medium focus on legal mechanisms to secure proprietary knowledge in organisations (50%) and the transfer of tacit knowledge, from current to future experts (50%). There was a lower focus on the retention of key employees through HR management mechanisms (25%). The participants also highlighted some additional areas to consider concerning modelling knowledge security. These were: the need for a balance between effective technology and a culture of sharing, instances of security being too stringent, a lack of focus on encouraging innovation by an organisation, awareness of the value of knowledge for malicious entities, and general issues that fit within the CIA triad paradigm.

From the perspective of model development, it will be important to identify security concept inputs, applicable in practice, and to be able to prioritise which of these components to focus on. In this case, these will include the need for the incorporation of governance, risk and compliance elements, the information security perspective, control mechanisms like archiving, legal, expert tacit knowledge transfer, and appropriate HR interventions. In terms of the additional considerations mentioned, the need for a balance between effective technology and

a culture of sharing will be important. This is because it highlights the need for strategic alignment between KM infrastructure and technologies as forming part of the broader KM solutions of an organisation. The balance of this relationship needs to be viewed from within the framework of the broader organisational context and focus. Additionally, two other elements will also need to be considered. Firstly, the correctly formulated balance between securing and sharing. Secondly, the recognition and identification of knowledge value as part of risk management processes and CIA triad considerations. These will form part of the balanced structure of any security controls implemented and will therefore be important to include.

From a knowledge security perspective, this will mean once again focusing on risk as a critical element of any approach to knowledge security. It will also mean considering information security concerning other knowledge security practices and their integration as part of KM. Thus, emphasis will need to be placed on the inclusion of control mechanisms like archiving critical knowledge, having appropriate legal protections in place, ensuring the transfer of expert knowledge, and retaining key employees as part of the broader set of available knowledge protection elements. In terms of the additional considerations mentioned, it will be important for an organisation to have their KM solutions well defined and implemented. The reason for this is to effectively meet their objectives based on the requirements of their knowledge context and focus.

The correctly formulated balance between sharing and security will also need to be considered, as governed by their strategic focus and determined by an effective analysis of risk. This will need to be thought of in terms of the organisation's knowledge risk profile. The same will apply when determining the value of knowledge, which will need to be considered in the collective, as part of any approach to risk mitigation. Further, considerations related to the balance of the CIA triad will need to form part of the application of any combined security controls implemented. Finally, these will also need to be framed by the organisation's knowledge risk profile and its objectives in terms of knowledge context, focus and strategy. Thus, the inputs related to risk management, information security elements, knowledge security controls, a balance between KM solutions and culture, a balance between security and KM objectives, and knowledge value considerations will be important in this regard.

7.3.3.7 Chapter 7 – Discussion and Inputs

The objective of the chapter was to provide a brief overview of conceptual models relating to knowledge security as discussed in Section 7.2.4. To begin, two points were illuminated as important to take into consideration when conceptualising knowledge security as discussed by Ilvonen and Ilvonen *et al.* Firstly, the need for the alignment of information security management activities with KM⁹⁹⁵. Secondly, the importance of a knowledge risk management model and a subsequent proactive approach to the management of self-contextualised knowledge security risk⁹⁹⁶. From this view, context is determined by decision and sense-making practices to achieve a greater level of understanding.

Next, two factors were also illuminated as important to take into consideration when conceptualising knowledge security as discussed by Elliot *et al.* Firstly, the importance of being able to strike a balance between sharing and protecting knowledge⁹⁹⁷. Secondly, the importance of context from both an inter and intra-organisational perspective. Context and the balance between sharing and protecting are discussed in terms of how they impact the organisational procedures needed to govern knowledge protection and sharing processes⁹⁹⁸. This was discussed in terms of the cost-benefit ratio based on knowledge value, acceptable risk, and risk mitigation factors such as sensitivity, trust, and legal protection mechanisms⁹⁹⁹.

From the perspective of model development, the illuminated factors of the need for alignment between information security management and KM, the importance of risk management and associated activities, organisational context and the balance between sharing and protecting will be important. Concerning the intersection between information security management and KM, even if taking a different view to that of Ilvonen, their approach still highlights the importance of aligning information security elements within a knowledge security approach. The emphasis on risk management and its associated elements is again important. This importance is because any security controls provided by information protection elements will need to be determined by an organisation's knowledge security risk assessments. From the perspective of context, this again will play a major role in helping to determine what knowledge is of value, how it is to be managed, shared and the implications for doing so. The use of any

⁹⁹⁵ As referenced in Section 7.2.4, paragraph 2.

⁹⁹⁶ As referenced in Section 7.2.4, paragraph 3.

⁹⁹⁷ As referenced in Section 7.2.4, paragraph 4.

⁹⁹⁸ As referenced in Section 7.2.4, paragraph 4.

⁹⁹⁹ As referenced in Section 7.2.4, paragraph 4.

mechanisms such as cost-benefit in the context of value and risk will be determined by the establishment of each organisation's definition of context. This, in turn, will help to determine what is seen as an acceptable balance between sharing and securing knowledge, based on their strategic requirements.

From a knowledge security perspective, these elements will form some of the core structures of any approach to securing organisational knowledge. These are discussed in terms of the alignment of security activities with KM, how relevant risks and mitigation strategies are determined and what applies to each organisation's context. This is in terms of their need for sharing or securing knowledge based on their own unique set of contextual requirements. Thus, the inputs of the alignment between information security and KM, the importance of risk and finally context in the determination of value and acceptable levels of sharing will be important in this regard.

7.3.4 Integrating Relevant Inputs into a Model

With the various inputs having been established, the next objective was to formulate the inputs into a conceptual model of knowledge security. Willemain¹⁰⁰⁰ advises that when it comes to developing the model structure, there can be a lot of switching between the different inputs. Willemain¹⁰⁰¹ goes on to discuss that this is something of a less formal procedure and generally requires experience, analytical ability, and a component of creativity. Since there is not one formally accepted method on how to do this, taking a looser approach is important as modellers should not be too constrained in their view¹⁰⁰². If the approach followed is too constrained, it could hinder creativity and the initial analysis¹⁰⁰³. Brooks and Wang¹⁰⁰⁴ point out that this means when models are developed by experts, they often consider various aspects of how the problem can be modelled. Through this process, they critically evaluate their ideas and further revise or develop the model iteratively according to their own set of requirements. This is not to say that there are no common practices that could be beneficial to follow, but rather that it is context and situation-specific as to what aspects of those common practices to consider.

¹⁰⁰⁰Willemain, 1995. *Model Formulation: What Experts Think About and When* p 916-932.

¹⁰⁰¹Willemain, 1995. *Model Formulation: What Experts Think About and When* p 916-932.

¹⁰⁰²Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1670.

¹⁰⁰³Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1670.

¹⁰⁰⁴Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1669.

To add some guidance, from the view of experts in practice, I examined the research done by Brooks and Wang¹⁰⁰⁵ on conceptual model development, in this case in the field of simulations. As part of their research, Brooks and Wang¹⁰⁰⁶ surveyed 102 experts to examine the different aspects of developing a conceptual model practically. Through their analysis, they identified several considerations and approaches those experts used, when developing their models. The main aspects that they identified can be categorised as: the modelling style used, the methods for understanding the real system and problem, the methods used for developing the initial conceptual model, and the methods used for documenting the conceptual model¹⁰⁰⁷. The most common sub-aspects relating to each of these main aspects used by experts in the field are summarised in Table 7-18¹⁰⁰⁸.

It should be noted that since Brooks and Wang's approach was based on the development of conceptual models in the field of simulations, not all aspects will apply to the context of KM and security. The aspects of interest for my purposes do not relate to the whole process of conceptual model development. Rather they relate to being able to get a better sense of the practical insights needed when integrating my identified inputs and representing them graphically. This forms part of the broader process of developing a conceptual model of knowledge security. Additionally, the aspects presented by Brooks and Wang are not a formalised method. Thus, they should rather be considered as a series of findings representative of the most common aspects in the field. Having made this distinction clear, the aspects that they outline still provide a useful base of ideas to consider. These considerations can be thought of in terms of the practical development of the conceptual model and the process of translating that into a diagrammatic representation.

Regarding the main aspects listed, several sub-aspects were found to be useful considerations for helping with the development of the conceptual model of knowledge security. These were taken and adapted to be in line with my context and objectives and to help me to better understand the practical process of representing the conceptual model graphically. Firstly, from

¹⁰⁰⁵Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1669-1685.

¹⁰⁰⁶Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1669.

¹⁰⁰⁷Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1673-1676.

¹⁰⁰⁸Brooks & Wang, 2015. *Conceptual Modelling and the Project Process in Real Simulation Projects: A Survey of Simulation Modellers* p 1673-1676.

Table 7-18: The Main Aspects Followed by Experts When Creating Conceptual Models

Main Aspect	Sub-Aspect
1.) The modelling style used (no percentages provided)	<ul style="list-style-type: none"> • Start small and add • Always draw/doodle • Make single model or make alternative models • Look at data first • Follow a systematic process
2.) The methods for understanding the real system and problem	<ul style="list-style-type: none"> • Analyse system data (74%) • Talk to management (69%) • Observe the system (53%) • Talk to system operators/servers (51%) • Talk to customers (35%) • Problem structuring method (30%) • Other (19%)
3.) The methods used for developing the initial conceptual model	<ul style="list-style-type: none"> • Previous experience of modelling a similar system or problem (71%) • Preliminary analysis of the system (e.g. simple analytical model) (64%) • Brainstorming session (43%) • Any other formal method (11%) • None of the above methods (6%)
4.) The methods used for documenting the conceptual model	<ul style="list-style-type: none"> • Process flow diagram (63%) • List of assumptions and simplifications (57%) • Logic diagram (31%) • Component list (22%) • Activity cycle diagram (19%) • UML (15%) • Other (4%) • None

the main aspect of the modelling style used, I chose to incorporate the ideas of starting small and adding to the model, drawing out many different versions of possible models on paper and making many alternative models. Secondly, from the main aspect of developing the initial conceptual model, I chose to incorporate the ideas of preliminary analysis of the system and brainstorming sessions. Lastly, the main aspects of understanding the real system and problem, and the methods used for documenting the conceptual model, did not produce any direct input

for my process but were rather more informative. For the aspect of understanding the real system and problem, the sub-aspects of this step had already been incorporated under the broader umbrella of my KM orientated modelling approach. For the aspect of the methods used for documenting the conceptual model, the findings were more relevant to modelling technical systems as opposed to management orientated knowledge and security issues. With these considerations in mind, I proceeded to develop and incorporate the identified inputs into a conceptual diagrammatic representation of knowledge security.

To do this, I aimed to frame the objective of what I was wanting to achieve with the model and to set limitations on the boundaries of what I was aiming to identify from the material. This was based on the context and scope of the research as defined by the primary research question. The limitations were set according to the objectives and outcomes of each chapter in line with the sub-research questions as outlined in Chapter 1. Each sub-research question dealt with a segment of the primary research question and therefore helped to form the scope from which the inputs for the model could be derived.

Thus, I began by firstly re-reading my initial draft chapters to refresh my grasp of the material. While doing so, I also highlighted and summarised the key points and outcomes from the individual chapters to get a broader overview of what I could consider as part of the construction of the diagrammatic representation of knowledge security. Following this, I took my initial summaries and identified the most obvious outputs of the chapters, in line with the broader research objectives. I then proceeded to begin the process of constructing a series of draft models. To do this, I began by brainstorming the possible combinations of inputs and various options and implications that arose from these combinations. Next, I took these ideas and began to draw out multiple versions of possible models on paper, including different alternatives for each model. I based this on the aspect of starting small and adding in additional details as required.

Once I had constructed enough draft models, by reaching a saturation point of no more unique ideas, I evaluated them for their fit with my research objectives. This was followed by a process of reduction consisting of two steps. Firstly, I eliminated models that were too far removed from my original objectives and framework. Secondly, I consolidated aspects and ideas from the different models to achieve a more inclusive draft version. I undertook this process by taking my paper drafts and consolidating them into a unified whole using concept mapping

software¹⁰⁰⁹. After this process was complete, I took the elements as presented in my concept map and further refined these into a preliminary draft model. Next, I examined how the different components of the model might best fit together, based on further analysis and critical thinking. Through this process, I arrived at the primary draft of my conceptual model. My objective in this regard was to construct the simplest model possible¹⁰¹⁰, one that was still representative enough to relate to practice. Using this principle, I further refined my primary draft and continued to simplify it as necessary.

Once this process was complete, I gave a draft version of the model to my supervisors for their inputs about the concept and considered any feedback that they provided. I also consulted with other academic experts, some of whom have extensive experience in developing models, to get additional insight into aspects of the modelling process that I may have forgotten to include. The experts did not observe or provide feedback on my actual model, but rather provided some tips and further reading material to consult. This allowed me to see how the process of conceptual modelling fits within the broader domain of scientific modelling, which I found useful for a couple of reasons. The first was that it helped me to better understand my position in the process of model development. The second was that it allowed me to better solidify my position within the broader approaches used.

Upon completion of the primary draft, with this information at hand, I proceeded to outline and refine the process related to the development of the final version of the model. This culminated in the development of the process outlined in Section 7.3 of this chapter. The final approach taken was framed in terms of its applicability to the field of KM and knowledge security. Through this process, I further refined my chapter summaries and examined them more critically to establish a summarised set of final model inputs as listed in Table 7-17. Once these had been established, I proceeded to overlay this final set of identified inputs with my draft model and added in any additional considerations. I again critically analysed my model to identify any gaps or anomalies in my representation that needed to be corrected. I also aimed to further simplify it based on the inputs and feedback I had obtained. This resulted in a few small adjustments and additions to the initial primary draft version I had created. Finally, I proceeded to turn the primary draft version of the model into a formal and final graphical representation of a conceptual model of knowledge security as a KM problem as shown in Figure 7-5. The details and relationships of the various components of my conceptual model

¹⁰⁰⁹ This was done using CMap Tools.

¹⁰¹⁰ Robinson, 2008. *Conceptual Modelling for Simulation Part 1: Definition and Requirements* p 278-290.

will be outlined in greater detail in Section 7.3.5. Some illustrative examples of the sub-concepts have also been provided in Table 7-19. These should by no means be considered comprehensive but are provided to rather help with a broader understanding of the concepts.

Figure 7-5: Conceptual Model of Knowledge Security Framed as a KM Problem

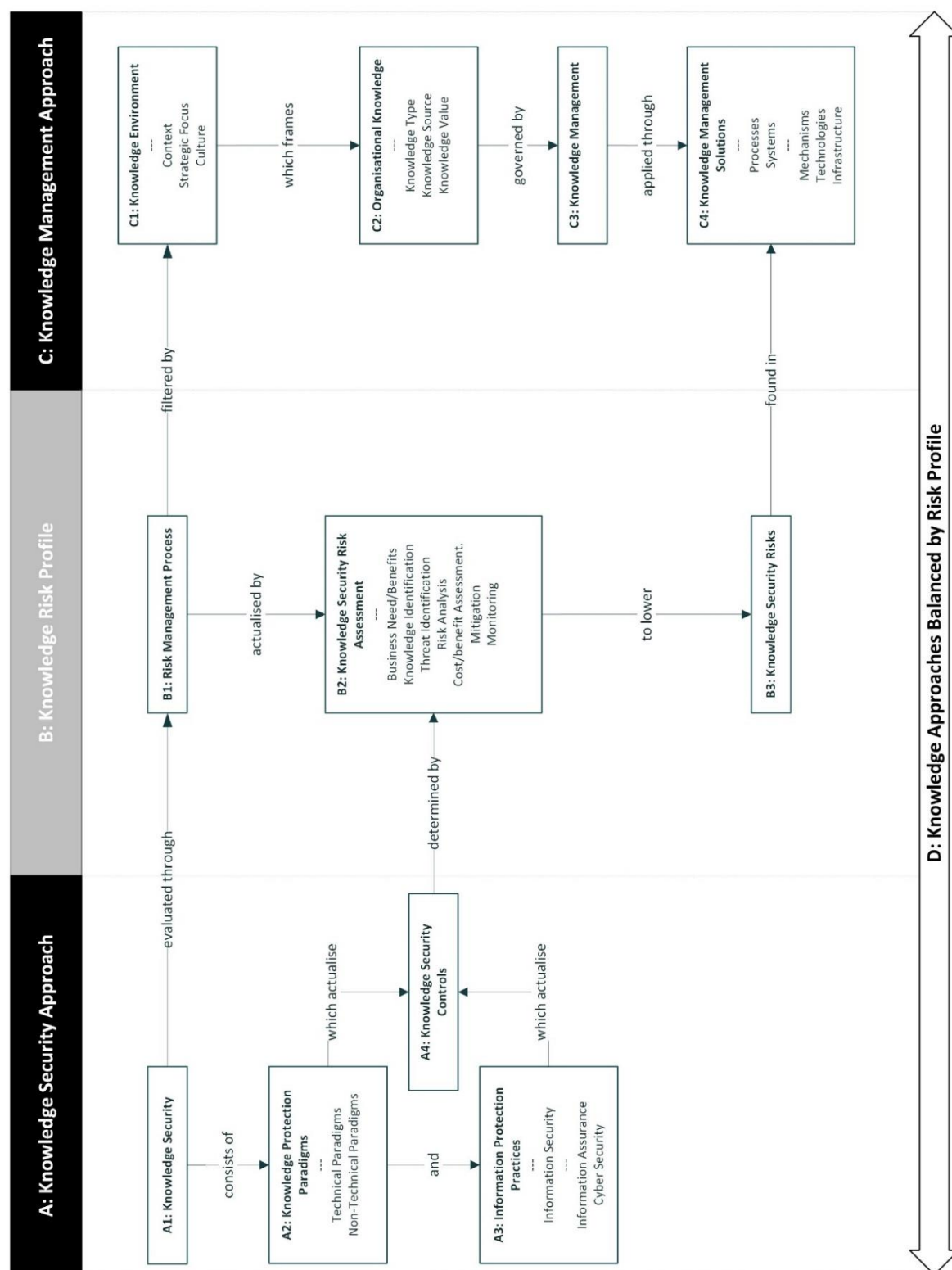


Table 7-19: Illustrative Examples of Model Sub-Concepts

Sub-Concepts	Illustrative Examples
A: Knowledge Security Approach	
A1: Knowledge Security	<i>See Section 7.3.5.1 Description of Concepts - A: Knowledge Security Approach</i>
A2: Knowledge Protection Paradigms	<p>Technical Paradigm Examples¹⁰¹¹:</p> <ul style="list-style-type: none"> • Systems Security... <p>Non-Technical Paradigm Examples¹⁰¹²:</p> <ul style="list-style-type: none"> • DIS Principles; Assurance; Risk...
A3: Information Protection Practices	<p>Information Security Examples¹⁰¹³:</p> <ul style="list-style-type: none"> • Security and Risk Management; Asset Security; Security Engineering; Communications and Network Security; Identity and Access Management; Security Assessment and Testing; Security Operations; Software Development Security... <p>Information Assurance Examples¹⁰¹⁴:</p> <ul style="list-style-type: none"> • Information Security Governance; Information Risk Management; Information Security Program Development and Management; Information Security Incident Management... <p>Cyber Security Examples¹⁰¹⁵:</p> <ul style="list-style-type: none"> • Frameworks and Standards; Physical Security; Risk Assessment; Governance; Threat Intelligence; User Education; Security Operations; Security Architecture...

¹⁰¹¹See Chapter 4, Section 4.3.3.2.¹⁰¹²See Chapter 4, Sections 4.3.3.1, 4.3.3.3 and 4.3.3.4.¹⁰¹³Brecht, 2019. *The CISSP CBK Domains: Information and Updates* [Online].¹⁰¹⁴Obbayi, 2019. *CISM: Overview of Domains* [Online].¹⁰¹⁵Jiang, 2017. *The Map of Cybersecurity Domains - Version 2.0* [Online].

Sub-Concepts	Illustrative Examples
A4: Knowledge Security Controls	<p>Knowledge Protection Controls¹⁰¹⁶:</p> <ul style="list-style-type: none"> Access controls; Automation Processes; Awareness and Training; Compliance Checks; Contingency Planning; Counterintelligence; Cultural Considerations; Employee Retention Mechanisms; Induction Processes; Innovation Processes; IP Protection; KMS Protection; Knowledge Approval; Knowledge Architecture; Knowledge Classification; Knowledge Depreciation Procedures; Knowledge Identification and Authentication; Knowledge Integrity; KM Processes; Knowledge Quality; Knowledge Refinement; Knowledge Security Governance; Knowledge Transfer Processes; Leadership Considerations; Legal Mechanisms; Mentoring; Monitoring; Risk Management; Policy; Political Engineering; Privacy Management; Records and Document Management; Role Management; Secure Communications; Strategic Management; Trust Management... <p>Information Protection Control Examples¹⁰¹⁷:</p> <ul style="list-style-type: none"> Access Controls; Awareness and Training; Audit and Accountability, Assessment; Authorisation and Monitoring; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Program Management; Personnel Security; Personally Identifiable Information Processing and Transparency; Risk Assessment; Systems and Services Acquisition; Systems and Communications Protection; Systems and Information Integrity; Supply Chain Risk Management...
B: Knowledge Risk Profile	
B1: Risk Management Processes	<i>See Section 7.3.5.3 Description of Concepts – B: Knowledge Risk Profile</i>

¹⁰¹⁶See Chapter 4, Section 4.3.3; Chapter 5, Section 5.4.1; Chapter 6, Section 6.3.5.

¹⁰¹⁷Joint Task Force, 2020. *Security and Privacy Controls for Information Systems and Organisations Rev 5*. p 428-465.

Sub-Concepts	Illustrative Examples
B2: Knowledge Security Risk Assessment	<p><i>Knowledge Security Risk Assessment Examples¹⁰¹⁸:</i></p> <p>Business Need/Benefits:</p> <ul style="list-style-type: none"> • Cost of Implementation; Expected Monetary Business Benefits <p>Knowledge Identification:</p> <ul style="list-style-type: none"> • Identify Communication Genres and Containers <p>Threat Identification:</p> <ul style="list-style-type: none"> • Identify Vulnerabilities and Motives to Exploit them; Identify Threat Agents <p>Risk Analysis:</p> <ul style="list-style-type: none"> • Identify Risks Connected to the Most Important Communication Genres; Analyse the Size of Risk and Costs of Risk Realisation; Identify Mitigation Means <p>Cost/Benefit Assessment.</p> <ul style="list-style-type: none"> • Business Benefits vs. Implementation Costs; Mitigation Costs vs. Mitigation Benefits <p>Mitigation:</p> <ul style="list-style-type: none"> • Implementation of Mitigation Means that are Deemed Reasonable <p>Monitoring:</p> <ul style="list-style-type: none"> • Set Triggers for Action; Any Change Should Trigger Re-evaluation of Business Need and Threats

¹⁰¹⁸Ilvonen *et al.*, 2015. *Knowledge Security Risk Management in Contemporary Companies - Toward a Proactive Approach* p 3944-3947.

Sub-Concepts	Illustrative Examples
B3: Knowledge Security Risks	<ul style="list-style-type: none"> • Unauthorised Access; Overload; Disasters; Espionage; Cultural Misalignment; Employee Loss; Lack of Innovation; Lack of Legal Protections; Incorrect Classification; Low Knowledge Integrity; Low Knowledge Quality; Ineffective Governance; No Transfer Processes; Lack of Leadership Support; Lack of Mentoring and Training; Ineffective Monitoring; Lack or Misalignment of Policy; Social Political Issues; Ineffective Records and Document Management; Lack of Role Management; Insecure Communications Channels; Ineffective Strategy; Trust Management Issues; Ineffective Risk Management; Cyber Attacks; Malware; Hacking; Breaches; Theft; Device Compromise...
C: Knowledge Management Approach	
C1: Knowledge Environment	<p>Context</p> <ul style="list-style-type: none"> • Industry Type; Project Duration; Project Complexity; Organisation Type; Knowledge Focus; Desired Outputs... <p>Strategic Focus</p> <ul style="list-style-type: none"> • Centralised KM Focus; Technical KM Focus; Social KM Focus; Level of Support Needed; Required Knowledge Use; Perceived Value; Perceived Importance... <p>Culture</p> <ul style="list-style-type: none"> • Level of Support for KM; Effectiveness of KM; Perceived Value; Perceived Importance; Impact of Knowledge Sharing...
C2: Organisational Knowledge	<p>Knowledge Type</p> <ul style="list-style-type: none"> • Explicit; Tacit; Implicit... <p>Knowledge Source</p> <ul style="list-style-type: none"> • Individuals; Groups and Teams, Structural Elements, Collective Memory... <p>Knowledge Value</p> <ul style="list-style-type: none"> • Perceived Value; Perceived Importance; Phase of Development; Refinement...
C3: Knowledge Management	<i>7.3.5.5 Description of Concepts – C: Knowledge Management Approach</i>

Sub-Concepts	Illustrative Examples
C4: Knowledge Management Solutions	<p><i>KM Solutions Examples</i>¹⁰¹⁹:</p> <p>KM Processes:</p> <ul style="list-style-type: none"> Knowledge Discovery Processes (Combination/Socialisation); Knowledge Capture Processes Externalisation/Internalisation); Knowledge Sharing Processes (Socialisation/Exchange); Knowledge Application Processes (Direction/Routines) <p>KM Systems:</p> <ul style="list-style-type: none"> Knowledge Discovery Systems; Knowledge Capture Systems; Knowledge Sharing Systems; Knowledge Application Systems <p>KM Mechanisms:</p> <ul style="list-style-type: none"> Analogies and Metaphors; Brainstorming Retreats; On-the-Job Training; Face-to-Face Meetings; Apprenticeships; Employee Rotation; Learning by Observation... <p>KM Technologies:</p> <ul style="list-style-type: none"> Decision Support Systems; Web-Based Discussion Groups; Repositories of Best Practices; Artificial Intelligence Systems; Case-Based Reasoning; Web Pages... <p>KM Infrastructure:</p> <ul style="list-style-type: none"> Organisational Culture; Organisational Structure; IT Infrastructure; Common Knowledge; Physical Environment
D: Knowledge Approaches Balanced by Risk Profile	
Underpins existing primary concept areas and sub-concepts	7.3.5.7 Description of Concepts – D: Knowledge Approaches Balanced by Risk Profile

7.3.5 Discussion and Implications

Concerning the conceptual model of knowledge security shown in Figure 7-5, the concepts are grouped under three primary concept areas. The three primary concept areas are: ‘A: Knowledge Security Approach’, ‘B: Knowledge Risk Profile’, and ‘C: Knowledge Management Approach’. A fourth primary element, ‘D: Knowledge Approaches Balanced by

¹⁰¹⁹Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 66-68.

Risk Profile’, underpins and emphasises the balance in the relationship needed between the other three primary concept areas. The alphanumeric codes assigned to each concept do not reflect the rank or importance of a concept but have been added for ease of reference when discussing the concepts and their relationships with one another. Three precursory issues need to be taken into consideration when reading the explanations to follow for each of the discussions related to the primary concept areas.

Firstly, there is a great deal of complexity that can be discussed relating to each concept and the composition of its possible elements, as relevant to many different types of organisations. However, given the scope of the research, in terms of time and space constraints, covering all possible complexity would be too broad. Therefore, it is important to note that I have not attempted to include every possible aspect or control related to each concept here. Rather, I have attempted to give a general sense of how the different concepts can relate to one another, particularly knowledge security and KM, keeping the primary research question in mind. The examples of any elements that I may provide, such as those in Table 7-19 related to the concepts, serve only as illustrative mechanisms. As such, they should not be considered in any way as a fully comprehensive list of all possible options available. Developing a comprehensive list will require further research and testing. To have any real meaning in that regard, it would also need to be related to the findings of the application of the model in practice. Thus, these aspects are beyond the scope of the current research project.

Secondly, if my model were to be followed in practice, it would likely be implemented differently than the way it has been outlined here, depending on the context and approach taken. For example, instead of outlining and discussing it sequentially from left to right, for clarity, it could be better to rather start with the risk environment and then expand out to the KM and security approaches as required. Taken as such, it would also require that any risk assessment begins with an initial set of questions related to identifying an organisation’s view of knowledge and its subsequent use of KM solutions. These aspects would also need to be considered within the broader context of its KM approach.

Thirdly, the model as I have discussed here will act as a framework upon which further aspects can be built concerning any knowledge security and management approaches taken. To do this, I have attempted to show how the relationship between knowledge security and KM can be better imagined. I have also attempted to frame this relationship around the interplay between the two areas and how this relates directly to securing KM activities in an organisation. Therefore, conceptually, this relationship requires a strong emphasis on knowledge risk which

acts as a fundamental link between the two approaches. In this regard, knowledge risk should be considered as part of the larger risk processes of an organisation in terms of its high-level governance and operational objectives.

Thus, with these considerations in mind, I will describe and discuss each of the model concepts in more detail. The description of the model concepts will be done without considering their relationships to one another, or their implications, to set a base level of understanding. Following the description of the model concepts, I will proceed to discuss their relationships more broadly and consider any implications that follow from this analysis. It should be noted that as the primary concept areas are interrelated, some overlap in points discussed will occur between the sections and concepts.

7.3.5.1 Description of Concepts – A: Knowledge Security Approach

A1: Knowledge Security – Is the starting concept under investigation and acts as a linking point between the knowledge security approach required and the evaluation of the knowledge risk profile as filtered by elements of the KM approach.

A2: Knowledge Protection Paradigms – Includes the possible technical and non-technical knowledge security paradigms relating to the protection of knowledge. Technical paradigms might include a focus on knowledge technologies and systems. Non-technical aspects might include a focus on DIS mechanisms, assurance issues and risk management implications.

A3: Information Protection Practices – Includes a focus on information security and its associated practices of information assurance and cyber security, focused towards protecting organisational information.

A4: Knowledge Security Controls – Are the combined controls used to secure organisational knowledge, as actualised by, and derived from the technical and non-technical knowledge protection paradigm mechanisms and the information protection practice mechanisms of information security, information assurance and cyber security.

7.3.5.2 Discussion of Concepts – A: Knowledge Security Approach

The primary concept area of ‘A: Knowledge Security Approach’ relates to the identified sub-concepts of ‘A1: Knowledge Security’, ‘A2: Knowledge Protection Paradigms’, ‘A3: Information Protection Practices’, and ‘A4: Knowledge Security Controls’. As identified in Chapter 3, in the context of the primary concept area, knowledge security can be summarised as having two main requirements: 1) The alignment of knowledge protection paradigms with

information security practices. 2) A linking of knowledge security with an organisations KM approach.

Firstly, concerning the alignment of knowledge protection paradigms with information security practices, a relationship between the two is required. This is important to be able to fully actualise an applicable set of knowledge security-focused controls. If this is not done, it could create some redundancy or missed gaps between knowledge security and information security controls. For example, Becerra-Fernandez and Sabherwal¹⁰²⁰ outline that an organisation's IT infrastructure is a critical component of its KM infrastructure too. As such, from an information security perspective, there are already standards guiding which controls can be used to protect this infrastructure. One possible standard that can be used in this regard is the National Institute of Standards and Technology's Special Publication 800-53 (NIST 800-53) on security and privacy controls¹⁰²¹. The NIST 800-53 standard lists an array of available security controls for this purpose. Therefore, broadly speaking it would not make sense to cover these controls again through knowledge security practices.

However, even with the application of an array of information security controls, some knowledge security gaps may still exist, even if focusing on the same area. These gaps would be due to the increased complications that manifest when managing knowledge as opposed to information, even in a technical sense. An example of this could be where the increased complexity associated with managing the rules and actions of a KMSs user base¹⁰²² exceeds the resource capacity of an information security team and overload occurs¹⁰²³. In this case, such a scenario could increase knowledge security risk if not managed effectively. Thus, security controls would need to be extended to include an algorithmic approach, managed through a mathematically driven framework, to automate these requests and reduce the associated complexity. Practically, this would manifest as ensuring better control over access to the system, privacy preservation in knowledge-extraction procedures, breaching awareness in the knowledge-dissemination procedures and abuse-accountability being incorporated as part of these additional considerations¹⁰²⁴.

¹⁰²⁰Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 66-68.

¹⁰²¹NIST, 2020. *Security and Privacy Controls for Information Systems and Organisations Rev 5*. p 428-465.

¹⁰²²Malatras *et al.*, 2005. *Secure and Distributed Knowledge Management in Pervasive Environments* p 79-83.

¹⁰²³Malatras *et al.*, 2005. *Secure and Distributed Knowledge Management in Pervasive Environments* p 79-83.

¹⁰²⁴Xu & Zhang, 2004. *PBKM: A Secure Knowledge Management Framework* p 1.

Thus, a balance and understanding from both an information security¹⁰²⁵, knowledge security¹⁰²⁶ and KM perspective¹⁰²⁷ are key in this regard. It is therefore important to collaborate on identifying the scope of controls available from a knowledge security perspective, based on the KM requirements determined by the knowledge environment. It is also important to establish if these elements are already covered by information security practices, or if they need to be included as complimentary or additional controls.

Secondly, concerning the linking of knowledge security with an organisation's KM approach, this is important as there is a need for balance and understanding. Balance and understanding will influence how knowledge security controls are chosen and to which KM solution areas they will be applied. Thus, there needs to be a link between the two, to identify and outline the fit of the security and KM requirements. This fit will largely be determined by the factors of influence related to the knowledge environment, with each organisation having a different focus as to what knowledge will be important to them. Practically, to define the level of balance and understanding needed, as per an organisation's knowledge security and KM approaches, a risk assessment process would need to be conducted to determine its risk profile. The composition of the risk management process, in the light of the knowledge risk profile, and its relationship to the knowledge security and KM approaches will be discussed in the next subsection.

7.3.5.3 Description of Concepts – B: Knowledge Risk Profile

B1: Risk Management Process – Is the central linking concept point between the knowledge security approach and the KM approach of an organisation in determining this association and balance through the establishment of a knowledge risk profile.

B2: Knowledge Security Risk Assessment – Is the risk assessment process followed to identify and determine the level of the security risk posed to an organisation's knowledge.

B3: Knowledge Security Risks – The collection of identified risks found that will negatively affect the security of an organisation's knowledge.

¹⁰²⁵Ryan, 2006. *Political Engineering in Knowledge Security* p 266.

¹⁰²⁶Park, 2006. *Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management – Results of a Delphi Study* p421.

¹⁰²⁷ Jennex & Durcikova, 2014. *Integrating IS Security with Knowledge Management: Are we Doing Enough to Thwart the Persistent Threat?* p 3457.

7.3.5.4 Discussion of Concepts – B: Knowledge Risk Profile

The primary concept area of ‘B: Knowledge Risk Profile’ relates to the identified sub-concepts of ‘B1: Risk Management Process’, ‘B2: Knowledge Security Risk Assessment’, and ‘B3: Knowledge Security Risks’. As identified in Chapters 3, 6 and 7, in the context of the primary concept area the knowledge security risk profile is presented as having two main requirements: 1) The establishment of a risk profile through the application of a risk assessment process to determine, manage and reduce knowledge risk. 2) To use the risk assessment process to create a link between the broader knowledge security approach and the KM approach based on a need for balance.

Firstly, concerning the establishment of a risk profile through the application of a risk assessment process to determine, manage and reduce knowledge risk, this is actualised by conducting a knowledge security risk assessment. The focus of the risk assessment process will be filtered by the view taken as to the organisation’s knowledge environment. This is because the knowledge environment will determine the focus of KM and how it is applied in an organisation. In turn, this will determine what is to be evaluated for risk and where possible risks may be identified. To be more effective in this regard, the risk assessment process followed would need to be focused on assessing knowledge. While many risk assessment frameworks could be used, I chose to incorporate the KSRM process as outlined by Ilvonen *et al.*¹⁰²⁸. I did so as the KSRM was developed specifically to focus on assessing knowledge security risks in organisations. If another risk assessment process is adopted, it would be important to adapt it to focus on knowledge security specifically. An alternative approach could also be to adopt a risk assessment process from a complementary field to knowledge security such as counterintelligence¹⁰²⁹. The use of a risk assessment from a counterintelligence view, in an organisation, would need to be framed from a business counterintelligence perspective, which already has a strong knowledge focus¹⁰³⁰.

Secondly, concerning using the risk assessment process to create a link between the broader knowledge security approach and the KM approach based on a need for balance, the risk profile of the organisation needs to be determined. To do so effectively, consideration first needs to be given to the KM approach taken by an organisation. This will be based on the factors

¹⁰²⁸ Ilvonen *et al.*, 2015. *Knowledge Security Risk Management in Contemporary Companies - Toward a Proactive Approach* p 3941-3950.

¹⁰²⁹ Ilvonen, 2013. *Knowledge Security - A Conceptual Analysis* p 106.

¹⁰³⁰ Shear, 2009. *Business Counterintelligence: Sustainable Practice or Passing Fad?* p 87.

contributing to its knowledge environment consisting of context, strategic focus, and culture. For example, this could mean considering factors such as the type of industry the organisation operates in; the duration and complexity of its projects; if it has a strategic KM focus that is centralised, technical or social; and how supportive its culture is to the idea of knowledge sharing. These factors will in turn influence how an organisation frames knowledge relating to its type, source, and value, which will be managed through an appropriate selection of applied KM solutions. The level of balance between sharing and securing will be determined by an organisation's leadership, relevant to these contextual needs. By determining the knowledge approach in this way, it can then be evaluated through the chosen risk management processes to determine where knowledge security risks reside. In turn, this will help to identify what knowledge security controls should be implemented to mitigate those risks. Thus, doing so will help to establish a balanced link between the broader knowledge security approach and the KM approach followed by an organisation. The composition of the KM approach, and its relationship with the knowledge risk profile and security approach, will be discussed in the next sub-section.

7.3.5.5 Description of Concepts – C: Knowledge Management Approach

C1: Knowledge Environment – Helps to define the KM approach taken through the evaluation of context, strategic focus, and culture as relating to the organisation. It also acts as a linking point between the different concepts of the KM approach and as a filtering mechanism for the evaluation of the knowledge risk profile.

C2: Organisational Knowledge – Is the primary asset of value that is enacted through sets of generalisations¹⁰³¹. This is achieved through the social and business processes of the organisation based on historically evolved collective understandings¹⁰³². Knowledge exists as different types and is found in a variety of sources within an organisation. How this is framed is determined by the knowledge environment, as the construct of the balance between these components will be different for each organisation.

C3: Knowledge Management – Is the management process of creating, sharing, and using organisational information and knowledge¹⁰³³. In this instance, it is governed by how

¹⁰³¹ Tsoukas & Vladimirou, 2001 *What is Organisational Knowledge* p 973.

¹⁰³² Tsoukas & Vladimirou, 2001 *What is Organisational Knowledge* p 973.

¹⁰³³ Girard & Girard, 2015. *Defining Knowledge Management: Toward an Applied Compendium* p 13.

organisational knowledge is defined and contextualised, as framed by the knowledge environment and applied through KM solutions.

C4: Knowledge Management Solutions – Consists of the collection of processes, systems, mechanisms, technologies, and infrastructure through which KM can be facilitated¹⁰³⁴. It is also the area where most knowledge security risks will be found. The application and composition of these solutions, and thus possible risks, are determined by an organisation's KM practices. These practices are framed within the broader context of the knowledge environment and are thus influenced by the KM approach followed.

7.3.5.6 Discussion of Concepts – C: Knowledge Management Approach

The primary concept area of 'C: Knowledge Management Approach' relates to the identified sub-concepts of 'C1: Knowledge Environment', 'C2: Organisational Knowledge', 'C3: Knowledge Management', and 'C4: Knowledge Management Solutions'. As identified in Chapters 1, 2, 3, 6 and 7, in the context of the primary concept area, the KM approach is presented as having two main requirements: 1) The evaluation of the knowledge environment and determining what is seen as knowledge. 2) The alignment between the knowledge security approach and the KM approach through the determination of risk.

Firstly, concerning the evaluation of the knowledge environment and determining what is seen as knowledge, it is important as it frames how an organisation will view and manage its knowledge. How knowledge is viewed will impact an organisation's KM approach and what KM solutions are applied to manage it. This is in terms of what types of knowledge they define, what sources of knowledge they identify, and the subsequent value seen to exist in this identified knowledge. These aspects will also help to determine the context in which any risk management processes will be conducted, and as such will help to link an organisation's KM approach to its knowledge risk profile. Within the knowledge environment, there are three framing aspects to consider; these being context, strategic focus, and culture.

The context of the organisation will impact how knowledge is viewed and managed through a variety of factors. These include elements such as the duration of projects, the type of organisation, its knowledge focus, the outputs produced and the variance in KM need. For example, as discussed in Chapter 6, for organisations with short-term projects, there may be an emphasis placed on capturing project and customer-related knowledge in a repository, while

¹⁰³⁴ Becerra-Fernandez & Sabherwal, 2010. *Knowledge Management: Systems and Processes* p 66-68.

for organisations with long-term projects, perhaps running for decades, they may have an additional need to retain or transfer tacit knowledge from key experts to future experts. Additionally, as also mentioned in Chapter 6, what is seen as knowledge by some organisations, may not be knowledge for another. This could relate to situations where a particular organisation needs to view collective meta-data as important knowledge; while for another organisation in a different context, this would not be considered knowledge in the traditional sense.

Next, the strategic focus of the organisation will influence how knowledge is viewed and managed. This is determined by the degree to which knowledge is needed to support an organisation's strategic objectives. In turn, this aspect will influence the degree to which knowledge is used, the value it holds, and the importance placed on managing it properly. From a strategic perspective, framing organisational knowledge by evaluating an organisation's knowledge environment will be important as it will determine what that knowledge is, how it is to be managed and what solutions need to be put in place to manage it.

The culture of an organisation will also play an important role in the effectiveness of KM and the value seen in adopting KM solutions. This will be particularly important regarding the impact on knowledge sharing. From this view, a culture that is supportive of KM but where KM solutions do not support that culture will limit the effectiveness of the KM approach. Conversely, a culture that is not supportive of KM but where there are KM solutions that would benefit a supportive culture will also limit the effectiveness of the KM approach. Thus, both aspects are related to cultural misalignment between the knowledge environment, KM, and the application of KM solutions, which could result in an increase in knowledge security risk through the failure of KM initiatives.

Secondly, concerning the alignment between the knowledge security approach and the KM approach, through the determination of risk, it is important as risk determination will help create an alignment between the two approaches. The alignment will be based on the view an organisation takes as to its knowledge environment. The view the organisation takes of its knowledge environment will also have a cascading effect. This concerns the framing and managing of organisational knowledge and to which KM solutions need to be implemented to achieve this. Thus, risk management processes will be needed to evaluate these KM solutions, as filtered by an organisation's knowledge environment. These processes will need to link back to the knowledge security approach to help determine the required set of knowledge security controls needed.

Without such an alignment, an imbalance could occur. If there is an imbalance, it could lead to a misalignment between what knowledge an organisation thinks is important to manage and protect and what is important for their knowledge context. For example, where a small organisation is critically reliant upon the expertise of a key director without whom they could not function. From a knowledge security perspective, the loss of the director would be catastrophic, as it would be a single point of failure from which the organisation may not recover. In such a case, the organisation may not realise the importance of the director for their knowledge security and may instead focus their attention on capturing key knowledge in a KMS. While this is important, more would need to be done to transfer the director's experience to others in the organisation through training and mentorship. It would also be important to institute measures to make sure the director is retained by the organisation and to assess the director's work activities through risk evaluation. Thus, the KM approach that an organisation follows will need to be aligned to its knowledge security approach. This needs to be balanced by its risk profile, which underpins and links the two aspects, as will be discussed in the subsection to follow.

7.3.5.7 Description of Concepts – D: Knowledge Approaches Balanced by Risk Profile

D: Knowledge Approaches Balanced by Risk Profile – Underpins all the concepts and the broader primary concept areas of the knowledge security approach, knowledge risk profile and KM approach. It represents the linking and interdependence of the different concepts. Additionally, it outlines too how there needs to be an association between the knowledge security approach and the KM approach taken. The link and level of balance between the two are thus determined by an organisation's knowledge risk profile.

7.3.5.8 Discussion of Concepts – D: Knowledge Approaches Balanced by Risk Profile

The primary concept area of 'D: Knowledge Approaches Balanced by Risk Profile' relates to all the other identified primary concept and sub-concept areas. As this primary concept area underpins the other primary concept areas, it does not have any additional sub-concepts contained under it. As identified in Chapters 3, 6 and 7, this primary concept area has one main requirement. This is to use the established risk profile as a key alignment and balancing mechanism between the knowledge security and KM approaches.

Thus, in terms of the alignment and balancing between the two approaches, it is important to do so as it ensures that there is a balanced link between knowledge security and KM activities. The relationship between the two is determined and maintained through an organisation's

knowledge risk profile. The risk process in turn helps to establish what knowledge security controls need to be in place to mitigate the identified risks. This is related to the application of KM solutions, based on the knowledge environment factors as outlined through the identified KM approach.

Concerning this balance, with the re-evaluation of risks as part of the KSRM cycle, it is important to note that the balance may change over time. This will be due to changes in the organisation's knowledge environment. In this sense, changes in the knowledge environment will act as a filter down factor in the determination of knowledge value and acceptable levels of sharing. It will also relate to how knowledge will be secured, as determined through the updated risk management profile. Such updates may be needed due to changes in the organisation's mandate, direction, services, strategic focus, or culture. Therefore, through using an organisation's knowledge risk profile, a link can be made between the objectives of knowledge security and the focus of the KM approach taken. In turn, this will help to align an organisation's security and KM objectives in a balanced way.

Finally, when referring to balance, it is important to note that I am not only talking about the balance needed in the application of the controls, for example, as would be filtered through security mechanisms like the CIA triad, when applying them to a specific KM solution. Rather, I am referring to the broader balance needed between the application of resources to aspects of knowledge security and KM approaches. How these resources are applied will have a direct impact on both the success of securing and sharing knowledge. From this view, it could mean either not devoting enough resources to protecting knowledge that is of value or devoting too many resources to knowledge that is of less value. Additionally, balance can also be considered from the view of the strategic balance needed between the objectives, relating to securing and sharing knowledge appropriately. In this regard, consideration is given to the broader security and KM functions of an organisation where misalignment between the security and KM objectives could increase their risks. The linking of objectives, and thus balance here, is therefore about identifying what to protect and at what level to protect it. How this is achieved practically will be up to each organisation based on its internal requirements and processes. Any determination of acceptable balance will also need to be done in consultation with an organisation's executive management, security, and KM professionals. The professionals will need to consider these factors relevant to those of their knowledge environment, as discussed in Chapter 6.

7.4 Limitations of the Model

While I have attempted to mitigate the effects of my research limitations, given the volume, complexity and project constraints associated with such research, there will be some limitations. Those that I have discussed already, relevant to other parts of the research in different chapters, will not be outlined again here. Rather, I will focus on discussing five further potential limitations as they relate to the development of the conceptual model of knowledge security as a KM problem.

Firstly, it is important to note that the model is purely theoretical at this stage. It has not been tested in practice either for refinement or practical application. As such, the model would need to be tested and refined further before any conclusions as to this approach's effectiveness and validity can be drawn.

Secondly, since I have aimed to develop this approach theoretically and conceptually, the examples or insights I have given in this chapter often have an element of conjecture associated with them. While they may make sense to me as the researcher, this view could differ greatly in practice or with the addition of more data. As I have not tested this, what looks reasonable to me may not look reasonable to someone else.

Thirdly, given the theoretical and conceptual nature of the model, I have aimed to treat it as more of a guide, one that would need to be tested practically. In my view, it has set the groundwork upon which more research could follow. After testing and expansion, if what I have presented here is found to be radically wrong in its approach, it could help set the direction for future research that tackles the problem from a more informed perspective.

Fourthly, as the model is theoretical and conceptual, and has not been tested and refined in practice, it should by no means be considered fully comprehensive. It is highly likely that upon conducting additional research related to the model, its aspects would be expanded upon. In addition, it may be found that they could also be constructed in a more logical way than what I have presented here.

Fifthly, the model that I have presented here is by no means the only way to approach this problem and may not even be the most effective. Without further testing, refinement, or development, I can only make determinations from the data which I have collected and framed from my own experience. Possible future approaches could be done with better ideas and a better understanding of how these relate to practice. While that which I have presented in this

dissertation is still of value and can be a useful contribution to the broader domain, and body of knowledge, it is important to keep this context in mind.

7.5 Recommendations for Future Research

While the model presented here has several limits, these limits also present the opportunity for more research to be conducted in the future. The model and the associated research that I have done here will be useful in this regard as it will provide a good starting base for future investigations. Three possible recommendations come to mind relating to the expansion and extension of the model and associated research.

Firstly, since the conceptual model has not been tested at this stage, this provides an opportunity to gather more data by testing and refining it in practice. This could be done by conducting more case studies, getting additional research input from a greater number of experts or even possibly some form of trials to test it in practice. Such an approach would help to alleviate many of the limitations mentioned above in Section 7.4.

Secondly, if the model could be tested and developed into a comprehensive representation of knowledge security, it could be expanded into a list of best practices or even a formal standard. Doing so could help to better define knowledge security requirements for an organisation's information security and KM teams and could be adopted as a compliance requirement by their assurance function.

Thirdly, the conceptual model could also be developed into a digital knowledge security risk assessment tool for organisations. For example, when initially considering ideas for the conceptual model, concerning the focus on risk, one of the drafts I created was a spreadsheet-based risk assessment process, which I did not complete. However, with further refinement of the model, this could easily be completed and structured into a digital self-assessment tool. The tool could remain purely as an add-on for spreadsheet software, or it could be expanded upon as stand-alone software or a web-based application. Additionally, the ideas of Monte Carlo simulation¹⁰³⁵ could be incorporated into it, or it could be combined with a fuzzy logic approach¹⁰³⁶ to add a predictive probability dimension. Unfortunately, given the limitations in the scope of this current research project, this is not possible to do here. After some exploratory

¹⁰³⁵ IBM Cloud Education, 2020. *Monte Carlo Simulation* [Online].

¹⁰³⁶ Stanford University, 2017. *Fuzzy Logic (Stanford Encyclopaedia of Philosophy)* [Online].

discussions and the development of some test cases, it could be an interesting area for a future research project.

7.6 Conclusion

Chapter 7 formed the final part of the research and aimed at examining how knowledge security can be modelled conceptually as a KM problem and be presented as a model. This was in line with the research question as mentioned in Chapter 1, Figure 1-2¹⁰³⁷. Thus, Chapter 7 consisted of a discussion around the process of conceptualising knowledge security as a KM problem and presenting it as a model. This formed the final part of the research project. The chapter began by selecting a conceptual modelling approach, through an examination of how conceptual modelling has been applied to KM. A conceptual modelling approach was compiled from the array of modelling approach factors identified. In addition, a brief examination of the literature was done relating to other conceptual models of knowledge security. This was necessary as several models of knowledge security had emerged in recent years since this project began. Apart from keeping up to date with developments in the literature, these models offered the possibility of gaining additional insights and potential inputs for my model. Next, the process of developing the conceptual model was outlined, discussed and the relevant actions were taken. These included establishing the objectives of the model, reviewing sources of information, extracting relevant model inputs, consolidating these inputs into a model, and discussing the model and its implications. Following this, the limitations of the model were briefly discussed and ideas for future research were presented.

¹⁰³⁷Research sub-question 6.1: *How can knowledge security be modelled conceptually as a KM problem and be presented as a model?*

Bibliography

- Academic Ranking of World Universities. (2019). *Shanghai global ranking of academic subjects 2020 - Library & information science / Shanghai ranking - 2020*. ARWU World University Rankings 2020 | Academic Ranking of World Universities. Retrieved April 3, 2020, Available: <https://www.shanghairanking.com/Shanghairanking-Subject-Rankings/library-information-science.html>
- Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, 42, 27-39.
- Ahmad, I., & Ewe, H. T. (2005, July). A model for secure knowledge sharing. In *Third International Conference on Information Technology and Applications (ICITA'05)* (Vol. 2, pp. 421-425). IEEE.
- AIIM. (2019). *What is information management?* AIIM - The Association for Intelligent Information Management. Retrieved July 18, 2019, Available: <https://www.aiim.org/What-is-Information-Management>
- Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, 25(1), 107.
- Al-Busaidi, Z. Q. (2008). Qualitative research and its uses in health care. *Sultan Qaboos University Medical Journal*, 8(1), 11.
- Ale, M. A., Chiotti, O., & Galli, M. R. (2005). A Distributed Knowledge Management Conceptual Model for Knowledge Organizations. *ICFAI Journal of Knowledge Management*, 3(4), 27-39.
- Al-Mualla, S. F. Tacit knowledge in organisations – towards an empirical inquiry.

- Ambrosini, V., & Bowman, C. (2001). Tacit knowledge: Some suggestions for operationalization. *Journal of Management Studies*, 38(6), 811-829.
- Argote, L., McEvily, B., & Reagans, R. (2003). Managing knowledge in organizations: An integrative framework and review of emerging themes. *Management Science*, 49(4), 571-582.
- Arnott, D., & Pervan, G. (2005). A critical analysis of decision support systems research. *Journal of information technology*, 20(2), 67-87.
- Arora, H., Mishra, B. K., & Raghu, T. S. (2006). Autonomic-computing approach to secure knowledge management: A game-theoretic analysis. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 36(3), 487-497.
- Azarpazhooh, A., Ryding, W. H., & Leake, J. L. (2008, December). Structured or unstructured personnel interviews? In *Healthcare management forum* (Vol. 21, No. 4, pp. 33-43). Sage CA: Los Angeles, CA: SAGE Publications.
- Bacon, F. (2014). *The New Organon*. Boston: Taggard and Thompson.
- Balci, O., & Ormsby, W. F. (2007). Conceptual modelling for designing large-scale simulations. *Journal of Simulation*, 1(3), 175-186.
- Beard, A. (2019, December 3). *Why cybersecurity isn't only a tech problem*. Harvard Business Review. Retrieved January 13, 2020, Available: <https://hbr.org/ideacast/2019/12/why-cybersecurity-isnt-only-a-tech-problem.html>
- Becerra-Fernandez, I., & Sabherwal, R. (2010). *Knowledge management: Systems and processes*. Routledge.
- Beckman, T. (1997). A methodology for knowledge management. International Association of Science and Technology for Development (IASTED). In *AI and Soft Computing Conference, Banff, Canada, 1997*.

- Beju, L. D., Brîndașu, P. D., & Oniță, G. V. (2013). A Conceptual Model of Product Design. In *Applied Mechanics and Materials* (Vol. 371, pp. 908-912). Trans Tech Publications Ltd.
- Bellinger, G., Castro, D., & Mills, A. (2004). Systems thinking: Data, information, knowledge, and wisdom.
- Bernard, H. R. (2011). *Research Methods in Anthropology: Qualitative and Quantitative Approaches*. Rowman Altamira.
- Bertino, E., Khan, L. R., Sandhu, R., & Thuraisingham, B. (2006). Secure knowledge management: confidentiality, trust, and privacy. *IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans*, 36(3), 429-438.
- Bevir, M., & Kedar, A. (2008). Concept formation in political science: An anti-naturalist critique of qualitative methodology. *Perspectives on Politics*, 503-517.
- Bharathi, S., & Suguna, J. (2014). A conceptual model to understand information security awareness. *International Journal of Engineering*, 3(8).
- Bhatt, G. D. (2001). Knowledge management in organizations: examining the interaction between technologies, techniques, and people. *Journal of knowledge management*.
- Bhatti, W. A., Zaheer, A., & Rehman, K. U. (2011). The effect of knowledge management practices on organizational performance: A conceptual study. *African Journal of business management*, 5(7), 2847-2853.
- Blackler, F. (1995). Knowledge, knowledge work and organizations: An overview and interpretation. *Organization Studies*, 16(6), 1021-1046.
- Boella, G., & Van Der Torre, L. (2006). Security policies for sharing knowledge in virtual communities. *IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans*, 36(3), 439-450.

- Bolisani, E., Scarso, E., & Zieba, M. (2015, April). How Small KIBS Companies Manage Their Intellectual Capital? Towards an Emergent KM Approach. In *European Conference on Intangibles and Intellectual Capital* (p. 25). Academic Conferences International Limited.
- Bontis, N. (2001). Assessing knowledge assets: a review of the models used to measure intellectual capital. *International journal of management reviews*, 3(1), 41-60.
- Boyles, J. E., Kirschnick, F., Kosilov, A., Yanev, Y., & Mazour, T. (2009). Risk management of knowledge loss in nuclear industry organisations. *International Journal of Nuclear Knowledge Management*, 3(2), 125-136.
- Brecht, D. (2019, June 30). *The CISSP CBK domains: Information and updates*. Infosec Institute Resources. Retrieved February 26, 2021, Available: <https://resources.infosecinstitute.com/certification/the-cissp-cbk-domains-info-and-updates>
- Brinkley, I. (2006). *Defining the knowledge economy*. The Work Foundation, London.
- Broda, S. (2005). *Intercultural challenges of knowledge focus strategy implementation in China* [Master's thesis]. http://www.gaoshan.de/kmchina/Stefan_Broda-Bachelor_Thesis.pdf
- Brooks, R. J., & Wang, W. (2015). Conceptual modelling and the project process in real simulation projects: a survey of simulation modellers. *Journal of the Operational Research Society*, 66(10), 1669-1685.
- Bunniss, S., & Kelly, D. R. (2010). Research paradigms in medical education research. *Medical education*, 44(4), 358-366.
- Burnette, M. (2017). Tacit knowledge sharing among library colleagues: a pilot study. *Reference Services Review*.

- Burrell, G., & Morgan, G. (2017). *Sociological paradigms and organisational analysis: Elements of the sociology of corporate life*. Routledge.
- Bygrave, W. D. (1989). The Entrepreneurship Paradigm (I): A Philosophical Look at its Research Methodologies. *Entrepreneurship Theory and Practice*, 14(1), 7-26.
- Cabrera-Suárez, K., De Saá-Pérez, P., & García-Almeida, D. (2001). The succession process from a resource-and knowledge-based view of the family firm. *Family Business Review*, 14(1), 37-48.
- Cabrera-Suárez, K., De Saá-Pérez, P., & García-Almeida, D. (2001). The succession process from a resource-and knowledge-based view of the family firm. *Family Business Review*, 14(1), 37-48.
- Carlsson, C., & Turban, E. (2002). Introduction: DSS: Directions for the next decade. *Decision Support Systems*, 33(2), 105-110.
- Cation, J. (2014, April 28). *Rithmio, aviculture, and inscites win big at 2014 cozad competition*. University of Illinois Urbana-Champaign - Grainger College of Engineering. Retrieved March 10, 2020, Available: <https://mechanical.illinois.edu/news/rithmio-aviculture-and-inscites-win-big-2014-cozad-competition>
- Cavana, R., Delahaye, B., & Sekeran, U. (2001). *Applied business research: Qualitative and quantitative methods*. John Wiley & Sons.
- Chalioiti, E. (2014). *Econ 483: economics of innovation & technology*. University of Illinois at Urbana-Champaign. Retrieved March 11, 2020, Available: https://files.webservices.illinois.edu/6443/econ483_sp14_chalioiti.pdf
- Chang-Albitres, C. M., & Krugler, P. E. (2005). A summary of knowledge management information gathered from literature, websites, and state departments of transportation.

- Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons.
- Chen, J., Ding, Y., & Wang, Q. (2009, December). The Third Category of Knowledge: Concept and Framework. In *2009 First International Conference on Information Science and Engineering* (pp. 4609-4612). IEEE.
- Chen, T. J., & Lee, J. S. (2004). *The new knowledge economy of Taiwan*. Edward Elgar Publishing.
- Cheung, C. F., Ma, R., Wong, W. Y., & Tse, Y. L. (2012). Development of an organizational knowledge capabilities assessment (OKCA) method for innovative technology enterprises. *International Journal of Economics and Management Engineering*, 6(7), 1698-1709.
- Chibelushi, C., & Costello, P. (2009). Challenges facing W. Midlands ICT-oriented SMEs. *Journal of small business and enterprise development*.
- Cho, T. (2011). *Knowledge management capabilities and organizational performance: An investigation into the effects of knowledge infrastructure and processes on organizational performance* (Doctoral dissertation, University of Illinois at Urbana-Champaign).
- Choo, C. W., Detlor, B., & Turnbull, D. (2000). WebWork: Information Seeking and Knowledge Work on the World Wide Web.
- Chrzanowska, J. (2014, July 9). *Demonstration qualitative interview - how it should be done* [Video]. YouTube. <https://www.youtube.com/watch?v=eNMTJTnrTQQ>
- Chua, I. S., Bogetz, A. L., Bhansali, P., Long, M., Holbreich, R., Kind, T., ... & Hirshfield, L. E. (2019). The patient experience debrief interview: how conversations with hospitalized families influence medical student learning and reflection. *Academic Medicine*, 94(11S), S86-S94.

- CIA. (2010, June). *Intelligence: open-source intelligence*. Central Intelligence Agency.
Retrieved March 24, 2020, Available: <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html>
- Clarke, T., & Clegg, S. (2000). Changing Paradigms: The Transformation of Management Knowledge for the 21st Century. *AUSTRALIAN JOURNAL OF PUBLIC ADMINISTRATION*, 59(3), 122-122.
- Clifford, N., French, S., & Valentine, G. (2010). *Key methods in geography*. SAGE.
- Coffey, A., & Atkinson, P. (1996). *Making sense of qualitative data: Complementary research strategies*. Sage Publications, Inc.
- Conner, K. R., & Prahalad, C. K. (1996). A resource-based theory of the firm: Knowledge versus opportunism. *Organization Science*, 7(5), 477-501.
- Conover, P. J., & Feldman, S. (1984). How people organize the political world: A schematic model. *American Journal of Political Science*, 95-126.
- Cope, J. (2005). Researching entrepreneurship through phenomenological inquiry: Philosophical and methodological issues. *International Small Business Journal*, 23(2), 163-189.
- Corney, P. (2013, January 11). Knowledge management is dead, but it won't lie down: A 10-year review of a KIM initiative. *knowledge et al | when the journey is as important as the destination*. <https://www.knowledgeetal.com/?p=465>
- Costa, P., Montenegro, R., Pereira, T., & Pinto, P. (2019). The security challenges emerging from the technological developments. *Mobile networks and applications*, 24(6), 2032-2037.

- Courtney, J. F. (2001). Decision making and knowledge management in inquiring organizations: toward a new decision-making paradigm for DSS. *Decision support systems*, 31(1), 17-38.
- Crabtree, B. F., & Miller, W. L. (1992). Doing qualitative research. In *Annual North American Primary Care Research Group Meeting, 19th, May, 1989, Quebec, PQ, Canada*. Sage Publications, Inc.
- Crane, L. (2013). A new taxonomy of knowledge management theory: the turn to knowledge as constituted in social action. *Journal of Knowledge Management Practice*, 14(1), 1-20.
- Cranfield, D. J., & Taylor, J. (2008). Knowledge management and higher education: A UK case study. *Electronic Journal of Knowledge Management*, 6(2).
- Creswell, J. W. (2009). *Research design: qualitative, quantitative, and mixed methods approaches* (No. Sirsi) i9781412965569).
- Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications.
- CSIAC. (2017). *Secure knowledge management workshop 2017 (skm 2017)*. CSIAC | Cyber Security and Information Systems Information Analysis Center. Retrieved January 13, 2020, Available: <https://www.csiac.org/event/secure-knowledge-management-workshop-2017-skm-2017/>
- Curado, C. M. M., Oliveira, M., & Maçada, A. C. G. (2011). Mapping knowledge management authoring patterns and practices. *African Journal of Business Management*.
- Darányi. (2011). *Discussion Workshop - The SHAMAN EU Project in a Nutshell: What next?* University of Borås. Högskolan i Borås - Högskolan i Borås. Retrieved March 15, 2020, Available: <https://www.hb.se/Global/HB%20->

[%20student/utbildningsområden/BHS/Dokument/Konferenser/Shaman%20workshop%202011.pdf](#)

Davenport, E., & Cronin, B. (2000). Knowledge management: semantic drift or conceptual shift? *Journal of Education for Library and Information Science*, 294-306.

Davenport, T. (2008). Enterprise 2.0: The new, new knowledge management? *Harvard Business Online*, 19.

Davenport, T. H. (1994). Saving IT's soul: Human-centered information management. *Harvard business review*, 72(2), 119-31.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

De Long, D., & Seemann, P. (2000). Confronting conceptual confusion and conflict in knowledge management. *Organizational Dynamics*, 29(1), 33-44.

Definitions.net. (2021). *What does conceptual model mean?* Retrieved January 20, 2021, Available: <https://www.definitions.net/definition/conceptual+model>

Department of Defence. (1999). *Department of defence joint course in communication - review of the literature*. The University of Oklahoma. Retrieved February 10, 2012, Available: <https://www.ou.edu/deptcomm/dodjcc/groups/02b1/02b1litreview.htm>

Desouza, K. C. (2006). Knowledge Security: An Interesting Research Space. *Journal of Information Science & Technology*, 3(1).

Desouza, K. C. (2007). *Managing knowledge security: strategies for protecting your company's intellectual assets*. Kogan Page Publishers.

Desouza, K. C., & Vanapalli, G. K. (2005). Securing knowledge in organizations: lessons from the defence and intelligence sectors. *International Journal of Information Management*, 25(1), 85-98.

- Desouza, K. C., & Vanapalli, G. K. (2005). Securing knowledge in organizations: lessons from the defence and intelligence sectors. *International Journal of Information Management*, 25(1), 85-98.
- DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, 40(4), 314-321.
- Dieng, R., & Corby, O. (Eds). (2003). *Knowledge Engineering and Knowledge Management. Methods, Models, and Tools: 12th International Conference, EKAW 2000, Juan-les-Pins, France, October 2-6, 2000 Proceedings*. Springer.
- Donnelly, R. (2019). Aligning knowledge sharing interventions with the promotion of firm success: The need for SHRM to balance tensions and challenges. *Journal of Business Research*, 94, 344-352.
- Dragicevic, N., Ullrich, A., Tsui, E., & Gronau, N. (2020). A conceptual model of knowledge dynamics in the industry 4.0 smart grid scenario. *Knowledge Management Research & Practice*, 18(2), 199-213.
- Drew, H. (2014). Overcoming Barriers: Qualitative Interviews With German Elites. *Electronic Journal of Business Research Methods*, 12(2).
- Drucker, P. F. (1999). Knowledge-worker productivity: The biggest challenge. *California management review*, 41(2), 79-94.
- Du Plessis, M. (2007). The role of knowledge management in innovation. *Journal of knowledge management*.
- Dubina, I. N., Carayannis, E. G., & Campbell, D. F. (2012). Creativity economy and a crisis of the economy? Coevolution of knowledge, innovation, and creativity, and of the knowledge economy and knowledge society. *Journal of the Knowledge Economy*, 3(1), 1-24.

- Dudovskiy, J. (2016). *The ultimate guide to writing a dissertation in business studies: a step-by-step assistance*. research-methodology.net.
- Eardley, A., & Uden, L. (Eds). (2010). *Innovative Knowledge Management: Concepts for Organizational Creativity and Collaborative Design: Concepts for Organizational Creativity and Collaborative Design*. IGI Global.
- Edvinsson, L., & Kivikas, M. (2007). Intellectual capital (IC) or Wissensbilanz process: some German experiences. *Journal of Intellectual Capital*.
- Edvinsson, L., & Malone, M. (1997). Intellectual Capital: Realizing Your Company's True Value by Finding Its Hidden Brainpower.
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, 14(4), 532-550.
- Elliott, K., Pataconi, A., Swierzbinski, J., & Williams, J. (2019). Knowledge protection in firms: A Conceptual framework and evidence from HP labs. *European Management Review*, 16(1), 179-193.
- Elliott, R., & Timulak, L. (2005). Descriptive and interpretive approaches to qualitative research. *A handbook of research methods for clinical and health psychology*, 1(7), 147-159.
- Farooq, R. (2019). Developing a conceptual framework of knowledge management. *International Journal of Innovation Science*.
- Felin, T., & Hesterly, W. S. (2007). The knowledge-based view, nested heterogeneity, and new value creation: Philosophical considerations on the locus of knowledge. *Academy of management review*, 32(1), 195-218.
- Fine, G. J. (1979). Knowledge and Logos in the Theaetetus. *The Philosophical Review*, 88(3), 366-397.

- Firestone, J. M., & McElroy, M. W. (2005). Doing knowledge management. *The learning organization*.
- Fitz-Gerald, Stuart J. (2008) Book Review of: 'Managing knowledge security: strategies for protecting your company's intellectual assets' by K.C. Desouza. *International Journal of Information Management*, 28(4), p. 342. ISSN (print) 0268-4012
- Foss, N. J., & Mahoney, J. T. (2010). Exploring knowledge governance. *International Journal of Strategic Change Management*, 2(2-3), 93-101.
- Fotache, M. (2005). Knowledge management between fad and relevance.
- Frost, A. (2010). *Knowledge management definition*. Knowledge Management Tools. Retrieved May 7, 2014, Available: <https://www.knowledge-management-tools.net/knowledge-management-definition.html>
- Gero, J. S. (1990). Design prototypes: a knowledge representation schema for design. *AI magazine*, 11(4), 26-26.
- Giedts, P. (2013). *Looking for a new name for knowledge management*. LinkedIn. Retrieved December 27, 2013, Available: <https://www.linkedin.com/groups/Looking-new-name-Knowledge-Management-47726.S.57192196>
- Girard, J., & Girard, J. (2015). Defining knowledge management: Toward an applied compendium. *Online Journal of Applied Knowledge Management*, 3(1), 1-20.
- Given, L. M. (Ed). (2008). *The Sage encyclopedia of qualitative research methods*. Sage publications.
- Global MIKE Study Group. (2018). *MIKE award: winners of the asian global mike award 2018 (in alphabetical order)*. <http://www.globalmikeaward.com/winner-list-2018.html> accessed 19-10-2020
- Global MIKE Study Group. (2019). *MIKE award: winners of the asian global mike award 2019*. <http://www.globalmikeaward.com/winner-list-2019.html> accessed 19-10-2020

- Gloet, M. (2006). Knowledge management and the links to HRM. *Management Research News*.
- Goddard, W., & Melville, S. (2004). *Research methodology: An introduction*. Juta and Company Ltd.
- Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. *Journal of management information systems*, 18(1), 185-214.
- Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems*, 21(2), 135-146.
- Gregory, F. (1993). Cause, effect, efficiency and soft systems models. *Journal of the Operational Research Society*, 44(4), 333-344.
- Guillemin, M., Barnard, E., Allen, A., Stewart, P., Walker, H., Rosenthal, D., & Gillam, L. (2018). Do research participants trust researchers or their institution? *Journal of Empirical Research on Human Research Ethics*, 13(3), 285-294.
- Gummesson, E. (2003). All research is interpretive! *Journal of business & industrial marketing*.
- Hacking, I., & Hacking, J. (1983). *Representing and intervening: Introductory topics in the philosophy of natural science*. Cambridge university press.
- Harris, D., Khan, L., Paul, R., & Thuraisingham, B. (2007). Standards for secure data sharing across organizations. *Computer Standards & Interfaces*, 29(1), 86-96.
- Harris, S. (2010). *CISSP All-in-One Exam Guide*, Columbus, Ohio.
- Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017, January). Case study research: Foundations and methodological orientations. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 18, No. 1).

- Hartley, J. F. (1994). Case studies in organizational research. *Qualitative methods in organizational research: A practical guide*, 208-229.
- Heckathorn, D. D. (2002). Respondent-driven sampling II: deriving valid population estimates from chain-referral samples of hidden populations. *Social problems*, 49(1), 11-34.
- Heemskerk, M., Wilson, K., & Pavao-Zuckerman, M. (2003). Conceptual models as tools for communication across disciplines. *Conservation Ecology*, 7(3).
- Helmy, Y. M., Abdelgaber, S., Fahmy, H., & Montasser, H. S. (2020). A conceptual ontological framework for managing the social business process to enhance customer experience. *Knowledge and Process Management*, 27(4), 262-271.
- Hemsley, J., & Mason, R. (2013). Knowledge and Knowledge Management in the Social Media Age, *Organizational Computing and Electronic Commerce*, 23(1-2), 138-167.
- Heron, J., & Reason, P. (1997). A participatory inquiry paradigm. *Qualitative inquiry*, 3(3), 274-294.
- Holsapple, C. (Ed). (2013). *Handbook on knowledge management 1: Knowledge matters* (Vol. 1). Springer Science & Business Media.
- Holsapple, C. W., & Joshi, K. D. (2000). An investigation of factors that influence the management of knowledge in organizations. *The Journal of Strategic Information Systems*, 9(2-3), 235-261.
- Hota, C., Upadhyaya, S., & Al-Karaki, J. N. (2015). Advances in secure knowledge management in the big data era. *Information Systems Frontiers*, 17(5), 983-986.
- Hughes, M. (2020). *Introducing the centre for corporate entrepreneurship and innovation*. Loughborough University. Retrieved March 20, 2020, Available: <https://www.lboro.ac.uk/departments/sbe/inspire/articles/issue18/ccei/>
- IAEA. (2006). *Risk management of knowledge loss in nuclear industry organizations*.

IBM. (2020, August 24). *What is monte carlo simulation?* IBM Cloud Learn Hub.

Retrieved January 1, 2021, Available: <https://www.ibm.com/cloud/learn/monte-carlo-simulation>

Ichikawa Jenkins, J., & Steup, M. (2017). The Analysis of Knowledge. *Stanford*

Encyclopedia of Philosophy. Stanford, CA: The Metaphysics Research Lab, Center for the Study of Language and Information, Stanford University.

Ilker, E. (2016). Comparison of convenience sampling and purposive sampling comparison of convenience sampling and purposive sampling. (February).

Ilvonen, I. (2013). Knowledge security-a conceptual analysis.

Ilvonen, I., Alanne, A., Helander, N., & Väyrynen, H. (2016, January). Knowledge sharing and knowledge security in finnish companies. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4021-4030). IEEE.

Ilvonen, I., Jussila, J. J., & Kärkkäinen, H. (2015). Towards a business-driven process model for knowledge security risk management: Making sense of knowledge risks. *International Journal of Knowledge Management (IJKM)*, 11(4), 1-18.

Ilvonen, I., Jussila, J., Kärkkäinen, H., & Päiväranta, T. (2015, January). Knowledge Security Risk Management in Contemporary Companies--Toward a Proactive Approach. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3941-3950). IEEE.

IMF. (2020). *IMF data mapper, gdp - current prices*. Retrieved March 20, 2020,

Available: https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADV_EC/WEOWORLD

Indiana University Bloomington. (2020). *Center for intellectual property law and innovation*.

IU Robert H. McKinney School of Law. Retrieved March 13, 2020,

Available: <https://mckinneylaw.iu.edu/ip/index.html>

ISchools. (2020, March 1). *About the ischools organisation*. iSchools, Inc.

Retrieved March 5, 2020, Available: <https://ischools.org/About>

Jasimuddin, S. M., Klein, J. H., & Connell, C. (2005). The paradox of using tacit and explicit knowledge: Strategies to face dilemmas. *Management decision*, 43(1), 102-112.

Jennex, M. E. (2014). A proposed method for assessing knowledge loss risk with departing personnel. *VINE: The journal of information and knowledge management systems*.

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, 9(5), 493-504.

Jennex, M., & Durcikova, A. (2014). Integrating IS security with knowledge management: Are we doing enough? *International Journal of Knowledge Management (IJKM)*, 10(2), 1-12.

Jennex, M., & Olfman, L. (2005). Assessing knowledge management success. *International Journal of Knowledge Management (IJKM)*, 1(2), 33-49.

Jiang, H. (2017, February 10). *The map of cybersecurity domains (version 2.0)*. LinkedIn.

Retrieved January 23, 2021, Available: <https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/>

Joia, L. A., & Lemos, B. (2010). Relevant factors for tacit knowledge transfer within organisations. *Journal of knowledge management*.

Joint Task Force. (2020). *Security and privacy controls for information systems and organizations rev 5: Draft NIST special publication 800-53 revision 5 (800-53 rev. 5)*.

National Institute of Standards and

Technology. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

Kakabadse, N. K., Kakabadse, A., & Kouzmin, A. (2003). Reviewing the knowledge management literature: towards a taxonomy. *Journal of knowledge management*.

- Kankam, P. K. (2019). The use of paradigms in information research. *Library & Information Science Research*, 41(2), 85-92.
- Kaplan, B., & Maxwell, J. A. (2005). Qualitative research methods for evaluating computer information systems. In *Evaluating the organizational impact of healthcare information systems* (pp. 30-55). Springer, New York, NY.
- Karagiannis, D., Buchmann, R., & Walch, M. (2017). How can diagrammatic conceptual modelling support knowledge management?
- Kerr, F. (2007). *Practical ways for competitive intelligence professionals to measure their success*. Knowledge management articles and resources from Knowledgepoint. Retrieved March 4, 2010, Available: https://www.knowledgepoint.com.au/business_intelligence/Articles/BI_CP004.html
- Kitfield, J. (2007, March 3). *Espionage, the Sequel*. Airforce Magazine. Retrieved January 8, 2007, Available: <http://www.afa.org/magazine/march2007/0307espionage.asp>
- Klein, D. A. (2009). *The strategic management of intellectual capital*. Routledge.
- Koeing, M. (2018, January 15). *What is km? Knowledge management explained*. KMWorld. Retrieved June 20, 2019, Available: <https://www.kmworld.com/Articles/Editorial/What-Is/What-is-KM-Knowledge-Management-Explained-122649.aspx>
- Kotiadis, K., Tako, A. A., & Vasilakis, C. (2014). A participative and facilitative conceptual modelling framework for discrete event simulation studies in healthcare. *Journal of the Operational Research Society*, 65(2), 197-213.
- Kulkarni, U. R., Ravindran, S., & Freeze, R. (2006). A knowledge management success model: Theoretical development and empirical validation. *Journal of management information systems*, 23(3), 309-347.

- Kuvik, A. N. (2015). *The global competition for talent: Life science and biotech careers, international mobility, and competitiveness* (Doctoral dissertation, Universiteit van Amsterdam [Host]).
- Kwek, V. (2000, December 18). *Review: the knowledge-creating company*. CSC Book Club. Retrieved August 6, 2013, Available: https://www.researchgate.net/profile/Miranda_Yeoh/post/Is_there_any_research_on_how_Japanese_companies_face_sustainable_development/attachment/59d61ea679197b807797d101/AS%3A279692067262469%401443695193479/download/18-Knowledge%2BCreating%2BCompany%2BSummary.pdf
- Lafuente, E., Solano, A., Leiva, J. C., & Mora-Esquivel, R. (2019). Determinants of innovation performance: Exploring the role of organisational learning capability in knowledge-intensive business services (KIBS) firms. *Academia Revista Latinoamericana de Administración*.
- Lee, J. B., & Rosenbaum, A. D. (2004). Knowledge management: Portal for corporate espionage? Part 2-Who spies? *Km World*, 13(1), 10-10.
- Lee, J., Upadhyaya, S. J., Rao, H. R., & Sharman, R. (2005). Secure knowledge management and the semantic web. *Communications of the ACM*, 48(12), 48-54.
- Lee, J., & Rosenbaum, A. (2003, November 1). Knowledge Management: Portal for Corporate Espionage? Defining the Problem Part 1. *KM World*. <https://www.kmworld.com/Articles/Editorial/Features/Knowledge-management-Portal-for-corporate-espionage-Part-1--9508.aspx>
- Leitch, C. M., Hill, F. M., & Harrison, R. T. (2010). The philosophy and practise of interpretivist research in entrepreneurship: Quality, validation, and trust. *Organizational Research Methods*, 13(1), 67-84.

- Leung, S. (2014, March 4). *Information school capstone research poster - forecasting the future of library leadership at the UW libraries*. Information School | University of Washington. Retrieved March 23, 2020,
Available: <https://ischool.uw.edu/capstone/projects/2014/forecasting-future-library-leadership-uw-libraries>
- Lewins, A., & Silver, C. (2007). Using Software in Qualitative Research: A Step-by-step Guide.
- Liu, S. (2002). *University of north carolina - introduction to knowledge management*. The University of North Carolina at Chapel Hill. Retrieved December 27, 2013,
Available: https://www.unc.edu/~sunnyliu/inls258/Introduction_to_Knowledge_Management.html
- Low, J. (2013). Unstructured and semi-structured interviews in health research. *Researching health: Qualitative, quantitative and mixed methods*, 2, 87-105.
- Maasdorp, C. (2001). Bridging individual and organisational knowledge: the appeal to tacit knowledge in knowledge management theory. In *International Symposium on the Management of Industrial and Corporate Knowledge*. (8^o, Compiègne 22-24 de octobre de 2001).
- Maier, R. (2005). Knowledge management systems: information and communication technologies for knowledge management. *Computing Reviews*, 46(1), 24.
- Malatras, A., Pavlou, G., Belsis, P., Gritzalis, S., Skourlas, C., & Chalaris, I. (2005, July). Secure and distributed knowledge management in pervasive environments. In *ICPS'05. Proceedings. International Conference on Pervasive Services, 2005*. (pp. 79-87). IEEE.
- Malwarebytes Labs. (2020). *State of Malware Report - 2020*.

- Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: a structured literature review. *Journal of Knowledge Management*.
- Mårtensson, M. (2000). A critical review of knowledge management as a management tool. *Journal of knowledge management*.
- Mason, J. (2002). Designing qualitative research. *Qualitative researching*, 2.
- McAfee, A. (2006, September). *Enterprise 2.0 inclusionists and deletionists*. Retrieved January 29, 2014, Available: http://andrewmcafee.org/2006/09/enterprise_20_inclusionists_and_deletionists/
- McGregor, D. (1971). Theory X and Theory Y" reprinted in DS Pugh, ed «, Organization Theory.
- Melnick, B. (2007). *Case study: Atlantis Systems International-Using KM principles to drive productivity and performance, prevent critical knowledge loss and encourage innovation* (No. IAEA-CN--153).
- Memon, N., & Daniels, T. (2007). Special issue on secure knowledge management. *Information Systems Frontiers*, 9(5), 449.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.
- Miller, B. F., & Keane, C. B. (1983). *Encyclopaedia and dictionary of medicine, nursing, and allied health*. WB Saunders Company.
- Mills, A. M., & Smith, T. A. (2011). Knowledge management and organizational performance: a decomposed view. *Journal of knowledge management*.
- Mills, J. H., Thurlow, A., & Mills, A. J. (2010). Making sense of sensemaking: the critical sensemaking approach. *Qualitative research in organizations and management: An international journal*.

- Mills, J., & Birks, M. (2014). *Qualitative methodology: A practical guide*. Sage.
- Milton, N. (2009, January 18). *What is Knowledge Management?* [Video]. YouTube. http://www.youtube.com/watch?v=x3qlftUB_Yg
- Morgan, A. (2005). Basic Guidance for Cross-Cutting Tools: Conceptual Models. *WWF Standards of Conservation Project and Programme Management, Resources for Implementing the WWF Standards*.
- Most Innovative Knowledge Enterprise. (2020). *About Us*. <http://menamikeaward.com/about-us/>. Retrieved October 14, 2020, Available: <https://menamikeaward.com/about-us/>
- Mouton, J. 2001. How to succeed in your master's and doctoral studies: A South African guide and resource book.
- Mukherjee, A. (2014). Patent protection under endogenous product differentiation. *Asia-Pacific Journal of Accounting & Economics*, 21(1), 78-93.
- Müller, H. (2014). *Knowledge Management* [PDF document]. Unpublished Informatics Class Notes.
- Mundy, D., & Chadwick, D. W. (2005). Secure Knowledge Management for Healthcare Organizations. In *Creating Knowledge-Based Healthcare Organizations* (pp. 321-336). IGI Global.
- Muniraman, C., Damodaran, M., & Ryan, A. (2007, April). Security and privacy issues in a knowledge management system. In *Proceedings of the 6th Annual Security Conference, Las Vegas, NV, USA*.
- Murphy, C. (2005). *Competitive Intelligence: Gathering, Analysing and Putting it to Work*. Gower Publishing, Ltd..
- Murray, P., & Myers, A. (1997). The facts about knowledge. *Information strategy*, 2(7), 29-33.

Murray, A. (2010, January 22). *As work changes, so must managers*. Wall Street Journal.

Retrieved September 14, 2014,

Available: <https://www.wsj.com/articles/SB10001424052748703699204575016981955854448>

Muswazi, M., & Nhamo, E. (2013). Note taking: a lesson for novice qualitative researchers. *Journal of Research & Method in Education*, 2(3), 13-17.

Myers, M. D. (2009). Qualitative research in business & management.

Mylopoulos, J. (1992). Conceptual modelling and Telos. *Conceptual modelling, databases, and CASE: An integrated view of information system development*, 49-68.

Ndlela, L. T., & Du Toit, A. S. A. (2001). Establishing a knowledge management programme for competitive advantage in an enterprise. *International journal of information management*, 21(2), 151-165.

Neef, D., Siesfeld, T., Siesfeld, G. A., & Cefola, J. (1998). *The economic impact of knowledge*. Routledge.

Nevo, D., & Chan, Y. E. (2007). A Delphi study of knowledge management systems: Scope and requirements. *Information & management*, 44(6), 583-597.

Newington, L., & Metcalfe, A. (2014). Factors influencing recruitment to research: qualitative study of the experiences and perceptions of research teams. *BMC medical research methodology*, 14(1), 1-11.

Newsire. (2000). Swiss real estate group, maag holdings, selects RSA keon and RSA SecurID to help secure knowledge management system. (2000, Apr 10). *PR Newsire* Retrieved Available: <http://ez.sun.ac.za/login?url=https://www-proquest-com.ez.sun.ac.za/wire-feeds/swiss-real-estate-group-maag-holdings-selects-rsa/docview/449355330/se-2?accountid=14049>

- Nonaka, I. (1991). The knowledge-creating company. *Harvard Business Review*, 69(6), 96-104.
- Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford university press.
- Nonaka, I., & Toyama, R. (2003). The knowledge-creating theory revisited: knowledge creation as a synthesizing process. *Knowledge Management Research & Practice*, 1(1), 2-10.
- Obbayi, L. (2020, October 15). *CISM: overview of domains*. Infosec Institute Resources. Retrieved February 23, 2021, Available: <https://resources.infosecinstitute.com/certification/cism-overview-domains/>
- O'Dell, C. S., O'dell, C., Grayson, C. J., & Essaides, N. (1998). *If only we knew what we know: The transfer of internal knowledge and best practice*. Simon and Schuster.
- Ogrean, C. (2006). Knowledge management—a source of sustainable competitiveness in the knowledge based economy.
- Padyab, A. M., Päivärinta, T., & Harnesk, D. (2014). Genre-Based Approach to Assessing Information and Knowledge Security Risks. *International Journal of Knowledge Management (IJKM)*, 10(2), 13-27.
- Park, I., Lee, J., Upadhyaya, S. J., & Rao, H. R. (2006). Part 2: emerging issues for secure knowledge management-results of a Delphi study. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 36(3), 421-428.
- Park, Y. S., Konge, L., & Artino, A. R. (2020). The positivism paradigm of research. *Academic Medicine*, 95(5), 690-694.

- Pathirage, C. P., Amaratunga, D. G., & Haigh, R. P. (2007). Tacit knowledge and organisational performance: construction industry perspective. *Journal of knowledge management*.
- Patton, M. Q. (2002). Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work*, 1(3), 261-283.
- Pennington, D. (2016). A conceptual model for knowledge integration in interdisciplinary teams: orchestrating individual learning and group processes. *Journal of Environmental Studies and Sciences*, 6(2), 300-312.
- Perry, C., Riege, A., & Brown, L. (1999). Realism's role among scientific paradigms in marketing research. *Irish Marketing Review*, 12(2), 16-23.
- Polanyi, M. (1966). The logic of tacit inference. *Philosophy*, 41(155), 1-18.
- Polanyi, M. (2015). *Personal knowledge: Towards a post-critical philosophy*. University of Chicago Press.
- Ponelis, S. R. (2011). *An exploratory study of business intelligence in knowledge-based growth small, medium and micro-enterprises in South Africa* (Doctoral dissertation, University of Pretoria).
- Ponelis, S. R. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of Information Systems research in small and medium enterprises. *International Journal of Doctoral Studies*, 10(1), 535-550.
- Popescul, D. (2011, June). The confidentiality–integrity–accessibility triad into the knowledge security. A reassessment from the point of view of the knowledge contribution to innovation. In *Proceedings of the 16th international business information management association conference (innovation and knowledge management, a global competitive advantage)* (pp. 1338-1345).

- Powell, W. W., & Snellman, K. (2004). The knowledge economy. *Annu. Rev. Sociol.*, 30, 199-220.
- Preston, J., Swan, J., Scarbrough, H., & Institute of Personnel and Development, London (United Kingdom);. (1999). *Knowledge management A literature review*.
- Prusak, L. & Snowden, D. (2008, July 6). *Is Knowledge Management Dead?* [Video]. Interview by P. Lambe. Gurteen. <http://www.gurteen.com/gurteen/gurteen.nsf/id/km-dead-lambe>
- Putter, A. P. (2018). *Knowledge Management for the South African Department of Defence* (Doctoral dissertation, Stellenbosch: Stellenbosch University).
- QS World University Rankings. (2020). *Library and information management*. Quacquarelli Symonds. Retrieved March 7, 2021, Available: <https://www.topuniversities.com/university-rankings/university-subject-rankings/2020/library-information-management>
- Quirkos. (2019, June 14). *Using semi-structured interviews in qualitative research* [Video]. YouTube. <https://www.youtube.com/watch?v=WgtLTSB6NIg>
- Randeree, E. (2006). Knowledge management: securing the future. *Journal of knowledge management*.
- Riesenberg, L. A., & Justice, E. M. (2014). Conducting a successful systematic review of the literature, part 1. *Nursing2020*, 44(4), 13-17.
- Robinson, S. (2008). Conceptual modelling for simulation Part I: definition and requirements. *Journal of the operational research society*, 59(3), 278-290.
- Robinson, S., Arbez, G., Birta, L. G., Tolk, A., & Wagner, G. (2015, December). Conceptual modeling: definition, purpose and benefits. In *2015 Winter Simulation Conference (WSC)* (pp. 2812-2826). IEEE.
- Rowley, J. (2002). Using case studies in research. *Management Research News*, 25(1), 16-27.

- Ruiz, C., Álvaro, G., & Gómez-Pérez, J. M. (2011, September). A framework and implementation for secure knowledge management in large communities. *In Proceedings of the 11th International Conference on Knowledge Management and Knowledge Technologies* (pp. 1-8).
- Russell, B. (2013). *Theory of Knowledge: The 1913 Manuscript*. Routledge.
- Russell, C. L. (2005). An overview of the integrative research review. *Progress in transplantation*, 15(1), 8-13.
- Ryan, J. J. (2006). Managing knowledge security. *Vine*.
- Ryan, J. J. (2006). Political engineering in knowledge security. *Vine*.
- Salazar, M. K. (1990). Interviewer bias: How it affects survey research. *Aaohn Journal*, 38(12), 567-572.
- Schank, R. C., & Abelson, R. P. (2013). *Scripts, plans, goals, and understanding: An inquiry into human knowledge structures*. Psychology Press.
- Science Direct. (2021). *Conceptual model*. ScienceDirect.com | Science, health and medical journals, full text articles and books. Retrieved January 20, 21, Available: <https://www.sciencedirect.com/topics/computer-science/conceptual-model>
- Sedighi, M., & Zand, F. (2012, November). Knowledge management: Review of the Critical Success Factors and development of a conceptual classification model. In *2012 Tenth International Conference on ICT and Knowledge Engineering* (pp. 1-9). IEEE.
- Senge, P. M. (1990). *The Fifth Discipline: the art and practice of the learning organization*.
- Serban, A. M., & Luan, J. (2002). Overview of knowledge management. *New directions for institutional research*, 2002(113), 5-16.
- Shear, C. J. (2009). *Business counterintelligence: sustainable practice or passing fad?* (Doctoral dissertation, Stellenbosch: University of Stellenbosch).

- Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *Vine*.
- Shelburne, W. A. (1988). *Mythos and logos in the thought of Carl Jung: The theory of the collective unconscious in scientific perspective*. Suny Press.
- Singh, R., & Salam, A. F. (2006). Semantic information assurance for secure distributed knowledge management: A business process perspective. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 36(3), 472-486.
- Singleton, R., & Straits, B. (2010). Approaches to social research/Royce A. Singleton, Jr., Bruce C. Straits.
- Skyrme, D. (1997). Knowledge management: making sense of an oxymoron. *Management insights*, 22.
- Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of knowledge Management*.
- Snowden, D. (2002). Complex acts of knowing: paradox and descriptive self-awareness. *Journal of knowledge management*.
- Snowden, D. (2009). *Defining knowledge management*. Cognitive Edge.
Retrieved December 17, 2014, Available: <https://cognitive-edge.com/blog/entry/3185/defining-km/>
- Spiro, R. J. (1988). Cognitive flexibility theory: Advanced knowledge acquisition in ill-structured domains. *Center for the Study of Reading Technical Report; no. 441*.
- Stanford University. (2017). *Fuzzy logic (stanford encyclopedia of philosophy)*. Stanford Encyclopedia of Philosophy. Retrieved February 22, 2021,
Available: <https://plato.stanford.edu/entries/logic-fuzzy/>

- Stellenbosch University. (2019). *Post graduate programmes in information and knowledge management* [Course overview]. Department of Information Science. <http://ikm.suinformatics.com/>
- Stellenbosch University. (2020). *Postgraduate skills development online training and courses* [Video]. Postgraduate Office Courses. <https://learn.sun.ac.za/course/view.php?id=56849>
- Stenmark, D. (2002, January). Information vs. knowledge: The role of intranets in knowledge management. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (pp. 928-937). IEEE.
- Syracuse University. (2018, May 14). *Syracuse intellectual property law institute*. Syracuse Intellectual Property Law Institute. Retrieved March 11, 2020, Available: <https://techcommercialization.syr.edu/academic-programs/>
- Takeuchi, H. (2001). Towards a universal management of the concept of knowledge. I. Nonaka ve D. Teece (Yay. Haz), *Managing industrial knowledge: Creation, transfer and utilization içinde* (ss. 315-329).
- Tampere University. (2020). *Profile, ilona ilvonnen: university instructor, information and knowledge management*. Etusivu | Tampereen korkeakouluyhteisö. Retrieved March 15, 2020, Available: <https://www.tuni.fi/en/ilona-ilvonnen#expander-trigger--field-research-fields>
- Teleos. (2015). *2015 Global most admired knowledge enterprises (make) report*. <https://www.coursehero.com/file/57295778/Executive-summary-2015pdf/>
- Teleos. (2016). *2016 Global most admired knowledge enterprises (make) report*. <http://www.kunskapsteknik.se/2016GlobalMAKE-ES.pdf>

- Teleos. (2017). *2017 Global most admired knowledge enterprises (make) report*. <http://docplayer.net/68790227-2017-global-most-admired-knowledge-enterprises-make-report.html>
- Terra, J. C., & Angeloni, T. (2003). Understanding the difference between information management and knowledge management. *KM Advantage*, 1-9.
- Thalheim, B. (2012). The science and art of conceptual modelling. In *Transactions on Large-Scale Data-and Knowledge-Centered Systems VI* (pp. 76-105). Springer, Berlin, Heidelberg.
- Thalmann, S., Manhart, M., Ceravolo, P., & Azzini, A. (2014). An integrated risk management framework: measuring the success of organizational knowledge protection. *International Journal of Knowledge Management (IJKM)*, 10(2), 28-42.
- The Hong Kong Polytechnic University & Arup University. (2020). *Hong Kong MIKE Award 2020*. Knowledge Management and Innovation Research Center. http://hkmikeaward.com/file/MIKE_briefing_session.pdf
- Thomas, J. C., Kellogg, W. A., & Erickson, T. (2001). The knowledge management puzzle: Human and social factors in knowledge management. *IBM systems journal*, 40(4), 863-884.
- Thuraisingham, B. (2004, September). Secure Knowledge Management. In *Secure Knowledge Management Workshop, Buffalo, New York, Sept.*
- Thuraisingham, B., & Parikh, P. (2008, December). Trustworthy semantic Web technologies for secure knowledge management. In *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (Vol. 2, pp. 186-193). IEEE.
- Times Higher Education. (2020, February 11). *World university rankings 2020*. Times Higher Education (THE). Retrieved March 5, 2020, Available: <https://www.timeshighereducation.com/world-university->

rankings/2020/world-

ranking#!/page/0/length/25/sort_by/rank/sort_order/asc/cols/stats

Trend Micro Research. (2019). *Mapping the future: dealing with pervasive and persistent threats, trend micro security predictions for 2019*.

Tsoukas, H. (1996). The firm as a distributed knowledge system: A constructionist approach. *Strategic management journal*, 17(S2), 11-25.

Tsoukas, H. (2002). Do we really understand tacit knowledge? Presented to Knowledge Economy and Society Seminar, LSE Department of Information Systems, 14 June 2002, Final draft to be included in Easterby-Smith, M. and M. Lyles (eds) (2003). *Handbook of Organizational Learning and Knowledge*.

Tsoukas, H. (2005). The firm as a distributed knowledge system: a constructionist approach. *Knowledge Management: Critical Perspectives on Business and Management*, 2, 30.

Tsoukas, H., & Mylonopoulos, N. (2004). Introduction: Knowledge construction and creation in organizations. *British Journal of Management*, 15(S1), S1-S8.

Tsoukas, H., & Vladimirou, E. (2001). What is organizational knowledge? *Journal of management studies*, 38(7), 973-993.

Tuomi, I. (2002). The future of knowledge management. *Lifelong learning in Europe*, 7(2), 69-79.

University of Amsterdam. (2016). *2-day course in entrepreneurship for master students (2 ects credits): how to successfully start a company or new venture*.

Retrieved March 15, 2020, Available: <https://www.uva.nl/en/shared-content/faculteiten/en/faculteit-der-geesteswetenschappen/events/courses/2016/04/2-day-course-in-entrepreneurship-for-master-students-2-ecs.html>

University of Illinois. (2020). *Intellectual property and technology law*. University of Illinois College of Law. Retrieved March 10, 2020, Available: <https://law.illinois.edu/faculty-research/specialty-programs/intellectual-property-and-technology-law/>

University of Illinois. (2020). *The iSchool at illinois: is 590ik explore information knowledge management Strategies*. School of Information Sciences. Retrieved March 11, 2020, Available: <https://ischool.illinois.edu/degrees-programs/courses/is590ik>

University of Nevada. (2019). *Writing and speaking center: how to use a concept matrix*. University of Nevada, Reno. Retrieved March 6, 2021, Available: <https://www.unr.edu/writing-speaking-center/student-resources/writing-speaking-resources/concept-matrix>

University of North Carolina. (2011). *Connecting clinical informatics and cancer outcomes research*. School of Information and Library Science. Retrieved March 10, 2020, Available: <https://sils.unc.edu/events/2011/cancer-outcomes>

University of North Carolina. (2012). *SILS alumna, meredith r. evans raiford appointed associate university librarian*. School of Information and Library Science. Retrieved March 10, 2020, Available: <https://sils.unc.edu/news/2012/meredith-raiford>

University of North Carolina. (2015). *Special course topic archive*. School of Information and Library Science. Retrieved March 10, 2020, Available: <https://sils.unc.edu/courses/special-topics/archive>

University of North Carolina. (2017). *Brewster kahle: "universal access to all knowledge"*. School of Information and Library Science. Retrieved March 10, 2020, Available: <https://sils.unc.edu/events/2017/brewster-kahle>

University of North Carolina. (2020). *Intellectual property clinic*. UNC School of Law. Retrieved March 10, 2020, Available: <https://law.unc.edu/experiential-learning/clinics/intellectual-property-clinic/>

University of Pennsylvania. (1113). *Systemic Reviews: Literature Search*. University of Pennsylvania Libraries. Retrieved October 21, 2019,

Available: <https://guides.library.upenn.edu/c.php?g=475980&p=3255414>

University of Sheffield. (2015). *Programme regulations finder, departments & services - law3020 intellectual property: patents, trade secrets*. The University of Sheffield. Retrieved March 13, 2020,

Available: <https://www.sheffield.ac.uk/programmeregulationsfinder/unit?code=LAW3020&org=SHEFFIELD&start=2012-09-24&loc=SHEFFIELD&cal=AUT%20SEM&year=2015>

University of Sheffield. (2019). *Programme regulations finder, departments & services - MGT376 international business*. The University of Sheffield. Retrieved March 13, 2020,

Available: <https://www.sheffield.ac.uk/programmeregulationsfinder/unit?code=MGT376&org=SHEFFIELD&start=26-Sep-2005&loc=SHEFFIELD&cal=SPR%20SEM&year=2019>

University of Sheffield. (2020). *Undergraduate prospectus law llb - property law (land law, equity and trusts)*. The University of Sheffield. Retrieved March 13, 2020,

Available: <https://www.sheffield.ac.uk/prospectus/courseDetails.do?id=M1002020>

University of Sheffield. (2020, February 15). *MSc human resource management with CIPD pathway modules*. Sheffield University Management School. Retrieved March 13, 2020, Available: <https://www.sheffield.ac.uk/management/modules/msc-human-resource-management-cipd-pathway-modules>

University of Sheffield. (2020, February 6). *General engineering - MGT388 finance and law for engineers*. The University of Sheffield. Retrieved March 13, 2020,

Available: <https://www.sheffield.ac.uk/meng-engineering/current/modules/mgt388>

University of Washington. (2020). *Intellectual property ll.m.* UW School of Law.

Retrieved March 9, 2020, Available: <https://www.law.uw.edu/academics/llm/ip>

University of Washington. (2020). *My plan: commld 558 law and policy (5)*. US School of Law. Retrieved March 9, 2020,

Available: <https://myplan.uw.edu/course/#/courses/COMMLD558>

Upadhyaya, S., Rao, H. R., & Padmanabhan, G. (2006). Secure Knowledge Management.

US News & World Report. (2017). *Best library and information science/studies programs*.

Retrieved May 23, 2019, Available: <https://www.usnews.com/best-graduate-schools/top-library-information-science-programs/library-information-science-rankings>

Van der Spek, R., & Spijkervet, A. (1997). *Knowledge management: dealing intelligently with knowledge*. Knowledge Management Network.

Vaughan-Nichols, J. (2019, July 18). *No love lost between security specialists and developers for linux and open source*. ZDNet. Retrieved July 20, 2019,

Available: <https://www.zdnet.com/article/no-love-lost-between-security-specialists-and-developers/>

Virtue, T., & Rainey, J. (2015). Information Risk Assessment. in " *HCISPP Study Guide*", Elsevier Inc.

Vissak, T. (2010). Recommendations for using the case study method in international business research. *Qualitative Report*, 15(2), 370-388.

Von Krogh, G. (1998). Care in knowledge creation. *California management review*, 40(3), 133-153.

Waheed, M., & Kaur, K. (2014). Knowledge quality: A review and a revised conceptual model. *Information Development*, 1, 14.

- Warwick University. (2019). *Information and data compliance - quick guide to information security at warwick*. Retrieved September 25, 2019,
Available: <https://warwick.ac.uk/services/idc/informationsecurity/training>
- Watson, I. (2002). Applying Knowledge Management: Techniques for Building Corporate Memories.
- Weaver, K., & Olson, J. K. (2006). Understanding paradigms used for nursing research. *Journal of advanced nursing*, 53(4), 459-469.
- Webster, F. (2006). Theories of the Information Society.
- Welman, C., Kruger, F., & Mitchell, B. (2005). Research Methodology (Third Edit). *Cape Town: Oxford University Press Southern Africa (Pty) Ltd.*
- Whitehead, S. (2001, September/October). The counterintelligence page: part 1. *The South African Security Professional*, 32.
- Wiig, K. M. (1994). *Knowledge Management Foundations: Thinking about Thinking-how People and Organizations Represent, Create, and Use Knowledge*. Schema Press, Limited.
- Wiig, K. M. (1997). Knowledge management: Where did it come from and where will it go?. *Expert systems with applications*, 13(1), 1-14.
- Wiig, K. M. (2000). Knowledge management: an emerging discipline rooted in a long history. *Knowledge horizons: the present and the promise of knowledge management*, 3, 26.
- Wikipedia. (2019). *Knowledge economic index*. Wikipedia, the free encyclopedia.
Retrieved January 8, 2020,
Available: https://en.wikipedia.org/wiki/Knowledge_Economic_Index

- Wikipedia. (2021). *Scientific modelling*. Wikipedia, the free encyclopedia.
- Retrieved January 26, 2021,
- Available: https://en.wikipedia.org/wiki/Scientific_modelling
- Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88, 101640.
- Willemain, T. R. (1995). Model formulation: What experts think about and when. *Operations Research*, 43(6), 916-932.
- Wood, D. (2016). Conceptual Models: Definition & Characteristics. Retrieved Available: <https://study.com/academy/lesson/conceptual-models-definition-characteristics.html>.
- Xu, J., & Quaddus, M. (2005). Exploring the perceptions of knowledge management systems. *Management Development*, 24(4), 320-334.
- Xu, S., & Zhang, W. (2004, September). PBKM: A secure knowledge management framework. In *Proc. NSF/NSA/AFRL Workshop Secure Knowledge Management*.
- Yadav, N., & Singh, S.P. (2013). A role of knowledge management in organizational performance. *Scientific & Engineering Research*, 4(1), 195-201.
- Yang, S. Y. (2001). Conceptions of wisdom among Taiwanese Chinese. *Journal of Cross-cultural psychology*, 32(6), 662-680.
- Yin, R. K. (2012). Case study methods.
- Yoo, S. J., & Huang, W. H. D. (2013). Employees' acceptance of knowledge management systems and its impact on creating learning organizations. *Knowledge Management & E-Learning: An International Journal*, 5(4), 434-454.
- Young, R. (2010). Knowledge management and innovation in a global knowledge economy. KM Egypt 2010, April 20–21. *Knowledge Associates International, London*.

- Zack, M. H. (1999). Developing a knowledge strategy. *California management review*, 41(3), 125-145.
- Zack, M. H. (1999). Managing codified knowledge. *Sloan management review*, 40(4), 45-58.
- Zanjani, M. S., Rouzbehani, R., & Dabbagh, H. (2008). Proposing a conceptual model of customer knowledge management: a study of CKM tools in British dotcoms. *management*, 7(8), 19.
- Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. *Journal of the American society for information science and technology*, 58(4), 479-493.
- Zurich Insurance Group. (2015). *Risk nexus overcome by cyber risks? economic benefits and costs of alternate cyber futures*. Atlantic Council.

Appendices – Appendix A

A Semi-Structured Interview Question Guide

A1 Overview of Knowledge Management

1. How do you define knowledge in your organisation?
2. What do you see as the objective of KM in your organisation?
3. What role does organisational culture play when it comes to KM in your organisation?
4. What role does organisational structure play when it comes to KM in your organisation?
5. What role does IT infrastructure play when it comes to KM in your organisation?
6. What role does common knowledge play when it comes to KM in your organisation?
7. What role does the physical environment play when it comes to KM in your organisation?

A2 Knowledge Discovery

1. Do you make use of any combination mechanisms to support knowledge discovery?
Examples include meetings, telephone conversations, documents, and the collaborative creation of documents.
2. Do you make use of any combination technologies to support knowledge discovery?
Examples include databases, web-based access to data, data mining, repositories of information, web portals, best practices and lessons learned.
3. Do you make use of any socialisation mechanisms to support knowledge discovery?
Examples include employee rotations across departments, conferences, brainstorming retreats, cooperative projects, and initiation.
4. Do you make use of any socialisation technologies to support knowledge discovery?
Examples include video conferencing, electronic discussion groups, chat, and e-mail.

A3 Knowledge Capture

1. Do you make use of any externalisation mechanisms to support knowledge capture?
Examples include models, prototypes, best practices, and lessons learned.

2. Do you make use of any externalisation technologies to support knowledge capture?
Examples include expert systems, chat groups, best practices databases and lessons learned databases.
3. Do you make use of any internalisation mechanisms to support knowledge capture?
Examples include learning by doing, on the job training, learning by observation and face to face meetings.
4. Do you make use of any internalisation technologies to support knowledge capture?
Examples include computer-based communication, artificial intelligence-based knowledge acquisition and computer-based simulations.

A4 Knowledge Sharing

1. Do you make use of any socialisation mechanisms to support knowledge sharing?
Examples include employee rotations across departments, conferences, brainstorming retreats, cooperative projects, and initiation.
2. Do you make use of any socialisation technologies to support knowledge sharing?
Examples include video conferencing, electronic discussion groups, chat, and e-mail.
3. Do you make use of any exchange mechanisms to support knowledge sharing?
Examples include memos, manuals, letters, and presentations.
4. Do you make use of any exchange technologies to support knowledge sharing?
Examples include team collaboration tools, web-based access to data, databases and repositories of information, best practices databases, lessons learned systems and expertise location systems.

A5 Knowledge Application

1. Do you make use of any direction mechanisms to support knowledge application?
Examples include traditional hierarchical relationships in organisations, help desks and support centres.
2. Do you make use of any direction technologies to support knowledge application?
Examples include capture and transfer of experts' knowledge, troubleshooting systems, case-based reasoning systems and decision support systems.
3. Do you make use of any routine mechanisms to support knowledge application?
Examples include organisational policies, work practices and standards.

4. Do you make use of any routine technology to support knowledge application?
Examples include expert systems, enterprise resource planning systems and management information systems.

A6 Examining Links Between Academia and Practice

1. Are security issues ever a consideration when it comes to KM in your organisation?
2. Do you pay any attention to intellectual property protection?
3. Do you make any efforts to retain people and/or their knowledge should they leave?
4. Is there any role played by information security in your KM practices?
5. Do you view the security of your knowledge as a contributing factor to your organisational performance?